

Om uberettiget adgang til "data" etter straffelovens § 145 annet ledd.

En kommentar over bruken av databegrepet i straffelovens § 145 annet ledd, og "uberettiget adgang", her under spørsmål om bruken av etikettering, med utgangspunkt i DVD-Jon dommen.

Kandidatnr: 351

Veileder: Jon Bing

Leveringsfrist: 9. mai 2005

Til sammen 17480 ord

11.05.2005

Innholdsfortegnelse

| | | |
|-----------------|---|------------------|
| <u>1</u> | <u>INNLEDENDE BEMERKNINGER OG AVGRENSNINGER.</u> | <u>1</u> |
| 1.1 | INNLEDNING | 1 |
| 1.2 | AVGRENSNING | 6 |
| 1.3 | DEN VIDERE GANGEN I OPPGAVEN. | 7 |
| <u>2</u> | <u>”DATA” I STRAFFELOVENS § 145 ANNET LEDD.</u> | <u>7</u> |
| 2.1 | ET KORT HISTORISK OVERBLIKK. | 7 |
| 2.2 | HVA ER OMFATTET AV ”DATA” I LOVENS FORSTAND? | 9 |
| 2.2.1 | HVA ER ”DATA”? | 10 |
| 2.2.2 | NEDRE GRENSE FOR DATABEGREPET. | 15 |
| 2.2.3 | KAN BESKYTTELSEN (CSS) VÆRE DATA? | 18 |
| 2.3 | DEKODERDOMMENE. | 20 |
| 2.3.1 | DEKODER DOMMENES TOLKNING AV ”DATA”. | 22 |
| 2.3.2 | DEKODERDOMMENES REKKEVIDDE. | 26 |
| <u>3</u> | <u>UBERETTIGET ADGANG.</u> | <u>27</u> |
| 3.1 | ”UBERETTIGET” | 28 |
| 3.2 | HVA FORSTÅR MAN MED UBERETTIGET? | 29 |
| 3.3 | HVA EN ER EN BESKYTTELSE. | 31 |
| 3.3.1 | HVILKE KRAV STILLES EN BESKYTTELSE | 32 |
| 3.3.2 | PÅ LIGNENDE MÅTE. | 34 |
| 3.4 | VIL BRUK AV DECSS KUNNE VÆRE BERETTIGET? | 36 |
| 3.4.1 | TILLATER ÅNDSVERKSLOVEN BRUK AV DECSS? | 37 |
| 3.4.1.1 | Hvor mye av verket kan kopieres? | 38 |
| 3.5 | SALG MED FORBUD MOT KOPIERING. | 41 |
| 3.5.1 | ETIKETTERING. | 43 |
| 3.5.2 | VEDTAGELSE AV EN ”SHRINK-WRAP” AVTALE. | 46 |
| 3.5.2.1 | Innholdsmessige mangler ved ”Shrink-wrap” klausuler. | 50 |
| 3.5.3 | ”CLICK-WRAP” AVTALER. | 51 |
| <u>4</u> | <u>OPPSUMERING.</u> | <u>52</u> |
| <u>5</u> | <u>LITTERATURLISTE</u> | <u>53</u> |
| <u>6</u> | <u>VEDLEGG.</u> | <u>57</u> |
| 6.1 | LB-2003-00731 – BORGARTING LAGMANNSRETT - DVD-JON DOMME | 57 |

1 Innledende bemerkninger og avgrensninger.

Jeg vil i det følgende se på noen av de spørsmål som reises i den populært kalte ”DVD-Jon dommen” eller bare DVD-dommen. Dommen ble avsagt av Borgarting lagmannsrett, 22.12.2003, etter først å ha gått for Oslo tingrett, TOSLO2002-00507 M/94. For enkelthets skyld har jeg lagt ved en kopi av dommen, som jeg har gitt nummererte avsnitt, som jeg vise til.

1.1 Innledning

Bakgrunnen til at jeg ønsket å behandle denne dommen er ikke bare dens potensielle relevans i dagens samfunn, men også den store oppmerksomheten den har vakt. Som uttalt av professor Gideon Parchomovsky¹, så er dette en av få norske dommer som har blitt kommentert i USA. Grunnen til dette er nok neppe dommens resultat som sådanne, men snarere det at det spørsmålet den omhandler er noe svært mange er opptatt av, ikke bare i Norge. På den ene siden har man opphavsmannen, eller den som representerer ham, som ønsker størst mulig beskyttelse for sitt verk og samtidig kunne utnytte det økonomisk. På den andre siden har man forbrukerne, som også ønsker å utnytte verket i størst mulig grad. Disse ønskene er ikke alltid sammenfallende.

Denne dommen viser også de utfordringer man kan bli stilt ovenfor når man beveger seg inn på et teknologisk komplisert område. Dette kan skape problemer for partene i retten, og for domstolen, å se kompleksiteten, samt de følgene dette kan få. Det samme vil kunne gjelde for lovgiver.

¹ Utalt i forelesningen ” External perspectives on the DVD-Jon Case” ved institutt for privatrett, 15.09.2004.

Dommen tar opp flere interessante spørsmål – noen som den behandler relativt grundig, og noen som i første øyekast kanskje blir forbigått eller kun nevnt i et åndedrag. DVD-dommen har også vært mye fremme i media, hvor den ofte har blitt feilaktig fremstilt. Man har sett uttalelser som ”Nå er det fritt frem å kopiere DVD-filmer, og spre dem på nettet.” Noen har vært ute i media og spådd film- og musikkbransjens fall.” Nå nylig, med forslag til endringer av åndsverkloven, har vi fått uttalelser den andre veien, om at ”MP3 blir forbudt!” Dette er med på å illustrere at det ikke bare er penger, men også følelser med i bildet. Man har for eksempel i media gitt åndsverksloven et kallenavn, ”MP3-Loven”.

Utgangspunktet for denne saken ligger i et datamaskinprogram laget av den tiltalte, på slutten av 90 tallet. Det fremkommer av faktum i dommen, at den tiltaltes ambisjoner var å lage et dataprogram som kunne spille av DVD-filmer under en av versjonene av operativsystemet Linux.² På tiden fantes det ikke et avspillingsprogram for DVD-filmer på Linux-plattformen. Det var noen problemer med å lage et avspillingsprogram for DVD-filmer for Linux. Et slikt program ville være relativt enkelt å lage. Hindringene lå i at Linux på tidspunktet ikke hadde støtte for filsystemet UDF, som DVD-film paten brukte, samt kopsisperren som finnes på de fleste DVD-filmer. Den sist nevnte vil hindre et avspillingsprogram å tyde dataen om ligger på DVD-platen. For å kunne spille av filmer, så må man ha tilgang til en nøkkel. Disse var og er fortsatt ikke offentlige tilgjengelige. Tilgang til disse kan fås ved å inngå en lisensavtale med DVD Copy Control Association Inc. (DVD-CCA). En slik avtale inneholder strenge betingelse for å få tilgang til en slik nøkkel, dette for å hindre at en slik hemmelig nøkkel skal bli offentlig kjent. Dette er lite forenlig med kontraktsgrunnlaget for distribusjon av Linux. Det sentrale i denne sammenheng er at all kildekoden til Linux-programmer skal være offentlig tilgjengelig. Dette skaper en situasjon hvor det ikke vil være mulig å lage et program for Linux som inneholder en avspillingsnøkkel for DVD-filmer, uten å komme i konflikt med lisensavtalen til DVD-CCA.

² Det finnes en rekke firmaer som distribuerer versjoner av operativsystemet Linux. F.eks. Redhat, SUSE og Mandrake. Det er noen forskjeller på distribusjonene, men de er alle fortsatt Linux i grunn.

DVD er en forkortelse for "Digital Versatile Disc", og ble laget med håp om at den skulle ta over rollen for den eldende CD standarden, samt å få eventuelt nye bruksområder. I dag har vi i all hovedsak tre grupper DVD'er. DVD-Rom for bruk til datamaskiner. Her har man også en serie standarder for skrivbare og overskrivbare DVD'er³. Som man kan oppservere, har man ikke oppnådd enighet om en standard, så inntil videre har man flere standarder.

Videre har man en DVD-Audio standard for musikk på DVD formatet. Dette var tenkt som en erstatning for musikk kompaktplaten, men man har ikke klart å overbevise forbrukeren om at det er på tide å bytte ut CD-spillere og CD samlingen.⁴ Til sist har man en DVD-Video standard, for visning av filmer. Denne var ment som en erstatter av video kassetten (VHS). Dette selv om man ikke kan ta opp fra fjernsyn til DVD.⁵ Det er den sist nevnte standarden, denne saken omhandler, og den standarden det blir vist til når man snakker om en DVD.

De aller fleste filmer som er utgitt på DVD formatet har implementert en form for kopibeskyttelse, Content Scrambling System, eller CSS. Dette var et system som ble påkrevd av filmselskapene for at de skulle godskjenne distribusjon av sine filmer på DVD. Dette fordi de mente at det forelå en betydelig fare for at filmene kunne bli ulovlig kopiert i en større skala enn før. Dette på grunn av at DVD er et digitalt medium. Kopieringen vil kunne skje raskere og billigere enn før. Kopien vil også lett kunne få en like god kvalitet som originalen, dette dog kun hvis ingen form for videre destruktiv kompresjon finner sted. Video og lyd tar opp mye lagringsplass. For å minske plassbruken kan man komprimere lyden og eller videoen. Normalt vil man kunne oppnå en kompresjon på rundt 1:2, for både lyd og bilde. Det vil si at en film kun vil ta opp halvparten av lagringsplassen av hva den originalt gjorde. Dette er imidlertid ikke alltid nok, så man velger da å bruke en destruktiv kompresjon. Her blir mye dataen, som man

³ De standardene som i dag finnes på markedet er; DVD+R (writeable), DVD+RW (rewriteable), DVD-R (samme som dvd+r, men et annet format), DVD-RW (samme som dvd+rw, men et annet format), DVD-RAM (random access memory), DVD-Video og DVD-Audio.

⁴ I dag er det også en annen standard som kjemper om å få bli neste generasjons musikk format, SACD (Super audio CD).

⁵ Det har i dag begynt å komme DVD-spillere med opptaksmulighet på markedet.

anser som overflødig slettet, i tillegg til den normale kompresjonen. Man vil kunne få en merkbar reduksjon i kvaliteten på lyd og bilde, men man vil lett kunne se en kompresjon rundt 1:10. Typiske former for slike formater er, Mpeg2, AC3⁶ og den velkjente mp3 formatet.⁷

På slutten av 90-tallet var det flere i Linux miljøet som arbeidet med å finne en løsning på avspillingsproblemet av DVD-filmer. Den tiltale var en av dem, og han var med på å utvikle et program som skulle kunne løse dette problemet. Det ferdige programmet kunne fjerne krypteringen⁸ fra filmen, for så å lagre filmen i ukryptert stand på datamaskinens harddisk. Fra harddisken kunne filmen så spilles av med ikke-autorisert utstyr. Dette resulterte også i at eksemplaret lett kunne kopieres på nytt og distribueres. Dette programmet fungerte kun i Windows. Det å skaffe støtte for filsystemet UDF, lot den tiltalte være opp til andre å løste.

Den tiltale er dog ikke tiltalt for å ha laget uautoriserte kopier av opphavsrettsbeskyttet materiale. Det er riktignok reist spørsmål om et mulig medvirkningsavnsvar kan forsvares. Det sentrale elementet i dommen er spørsmålet om det har blitt foretatt en omgåelse av en sikkerhetsforanstaltning, og om den tiltalte så har skaffet seg en uberettiget adgang til filmen.

Lagmannsretten tar utgangspunkt i bakgrunnen til at det finnes kopibeskyttelse på DVD-filmer. Det er en mer eller mindre berettiget frykt, fra filmselskapenes side, for at ulovlig kopiering av filmer skal være med på å undergrave inntektspotensialet som en film representerer. Problemstillingen er ikke ny. Det som har vært med på å aktualisere dette problemet, er at filmene det her er snakk om er lagret på et digitalt medium, DVD-platen. Dette medfører at det er teoretisk mulig å lage en kopi som er identisk med originalen, og sist men ikke minst at man kan fremstille kopier raskt og relativt rimelig.

⁶ Mpeg2 er det komprimerte formatet for film på dvd. AC3 er formatet som brukes på lydsporet

⁷ Mpeg-layer3, originalt en standard for lyd på Video-CD, og planlagt til å være standarden for lyd på DVD-filmer i Europa, i et forsøk på å skille filmer for de amerikanske og Europeiske markedene

⁸ Ved kryptering, så gjøres data uleselig. Ved å oppgi rett nøkkel, kan man allikevel gjøre dataen lesbar.

Disse egenskapene blir da med på å forsterke frykten for at ulovlige kopier skal bli gjort tilgjengelig for en billig penge, og stjele markedsandeler fra de rettmessige kopiene.

For å prøve å hindre en slik utvikling, valgte Motion Picture Association⁹ å etablere en stiftelse som skulle ha til formål å administrere og jobbe for sikkerhet for filmer på dvd-mediumet. Stiftelsen fikk navnet, DVD Copy Control Association Inc. Man utviklet så en måte å beskytte filmer mot kopiering gjennom å kryptere innholdet. Koden som ble laget ble kalt Content Scrambling System, eller CSS. Det er for å ha brutt denne, den tiltalte har blitt stevnet for retten.

Retten nevner også at det finnes en form for sonekoding på dagens filmutgivelser. Dette kan allikevel neppe bli sett på som en kopibeskyttelse. Dette blir det også tatt til orde for i forarbeidene til de kommende endringer i åndsverksloven, hvor det uttales;

”(...) såkalte sonefrie DVD-spillere ikke omfattes av andre ledd, da regionskodingen ikke kan anses anvendt for å kontrollere bruk som er omfattet av de opphavsrettslige eneretter.”¹⁰

Dette er nok mer et markedsføringstrekk fra filmbransjens side. Man ønsker for eksempel å se hvordan en film blir tatt imot i USA før den slippes i Europa. Det kan også være et ønske om å ha kontroll på når filmene kommer til forskjellige markeder. Dette for å forhindre at forskjellige filmer skal komme til å konkurrere med hverandre. Da spesielt med tanke på selskapets egne filmer. For det andre er sonekodingen heller ikke utformet for å hindre kopiering. Det den skal hindre er avspilling. Den virker slik at man har delt verden inn i forskjellige soner. For eksempel er USA sone 1 og Europa sone 2. Hvis man har en avspiller kjøpt i Europa, så skal man kun kunne avspille filmer kjøpt i Europa, og ikke filmer fra USA. Man ser dog i dag at nærmest alle spillere som selges har mulighet til å avspille filmer fra alle soner. I praksis så blir soneordningen et mye mindre hinder for avspilling, enn for eksempel forskjellen på fjernsynsstandardene

⁹ Dette er en organisasjon som representerer de fleste større amerikanske filmselskapene.

¹⁰ Ot.prp.nr.46 side 155 høyre spalte 5 avsnitt.

for USA og Europa, henholdsvis NTSC og PAL.¹¹ Man vil ikke kunne vise en film laget for et amerikansk fjernsyn på et europeisk, eller motsatt. I beste fall vil man få filmen i sort/hvitt, og i feil hastighet. Man har dog etter hvert fått fjernsyn som kan vise begge standarder, men dette er ikke alltid tilfelle for de billigste versjonene.

Retten legger videre til grunn at piratkopiering ikke har vært noe mål for tiltalte, når han var med på å utvikle programmet DeCSS¹². Bakgrunnen for denne assumpsjonen er at da programmet ble laget, var det ikke noen praktiske måter å overføre eller lagre en eventuelt kopiert DVD-film på. Det ville la seg gjennomføre, men det ville bli dyrere enn å faktisk kjøpe filmen. Videre ble det vist til logger over samtaler den tiltalte hadde hatt med andre, hvor han tar avstand fra en slik piratvirksomhet.

Retten nevner også, det som kanskje er filmbransjens største problem når det gjelder ulovlig kopiering av opphavsrettsbeskyttet material. Det er problemet med at legale produsenter av DVDer, også produserer illegale kopier om natten, i de samme lokalene som de jobber legalt i om dagen. Kopibeskyttelsen, CSS, vil neppe være til hinder for en slik organisert og profesjonell kopiering. De sitter jo også tross alt med en original, laget for kopiering. Denne kopsisperren er nok laget for å hindre kopiering i det private markedet.

1.2 Avgrensning

Spørsmålet om medvirkning kommer opp i DVD-dommen i form av det stilles spørsmål om bruk av den tiltaltes datamaskinprogram kan likestilles med at den tiltalte har medvirket. Spørsmålet blir ikke behandlet utover at domstolen ikke finner at det er ført bevis for at medvirkning har funnet sted. Jeg vil således heller ikke i denne avhandlingen gå inn på spørsmålet om medvirkning.

¹¹ NTCS har en billedoppløsning på 480 horisontale linjer, og viser 30 bilder i sekundet. PAL har en oppløsning på 576 linjer og viser 25 bilder per sekund.

¹² En forkortelse for De Content Scrambling System. Altså et CCS fjerningsprogram.

Jeg vil også avgrense min avhandling mot spørsmålet om omvendt utvikling eller dekompilering. Dommen vurderer ikke spørsmålet ut over å si at det ikke er ført tilstrekkelig bevis for dette. I denne sammenheng ville det også ha oppstått spørsmål om etter hvilket lands rett man skal løse dette problemet.

Jeg har nylig blitt gjort kjent med at det skal ha blitt foretatt en revidering av straffelovens § 145 annet ledd. Jeg har forsøkt å finne denne, men i skrivende stund (28.4.05) har jeg ikke klart å finne den, verken på lovdata eller andre steder. Jeg ser meg dermed nødt til å avgrense mot en slik endring.

1.3 Den videre gangen i oppgaven.

Jeg har delt oppgaven inn i to hoveddeler. Først vil jeg ta for meg databegrepet i straffelovens § 145 annet ledd, her under hvordan dette ble håndtert i DVD-dommen. Deretter vil jeg se hvordan ”data” blir forstått av Høyesterett i dekomplerdommene.

I oppgavens andre del vil jeg ta utgangspunkt i hva som ligger i begrepet ”uberettiget” i straffeloven § 145 annet ledd.

2 ”Data” i straffelovens § 145 annet ledd.

2.1 Et kort historisk overblikk.

Når straffeloven ble vedtatt i 1902, inneholdt § 145 en tilsvarende regel som i dag, men da naturlig nok, med en litt annerledes ordlyd. Den rammet da den som ”(...) uberettiget bryder Brev eller andet lukket Skrift eller baner seg Adgang til en andens tillaaede gjenstander.”.

I 1958 ble det tilføyd en utvidelse av bestemmelsen til også å verne fortrolig utveksling av muntlig informasjon.

I 1979 ble det foretatt endringer i straffeloven i et ledd i å implementere den europeiske konvensjon 27.01.1977 om nedkjemping av terrorisme. Noe av det man ønsket å få regulert var såkalt ”Wiretapping”.¹³ Man fikk så et nytt annet punktum i § 145. Denne utvidelsen lød:

”Det samme gjelder den som uberettiget skaffer seg adgang til innholdet av en lukket meddelelse eller opptegnelse når dette regulært bare er tilgjengelig ved hjelp av særskilt utstyr for tilkopling, avspilling, gjennomlysning, avlesning eller liknende.”

Her ser man at lovgiver presiserer at, lovbestemmelsen også omfatter meddelelser som er lagret med hjelp av, da nyere teknologi, som for eksempel mikrofilm, båndopptagere, teleks med mer.

Vi fikk en videre endring i 1987. Dette kom som en følge av et arbeid som startet i 1983, hvor Straffelovrådet fikk i oppdrag å kartlegge former for datakriminalitet.¹⁴ Man ønsket med dette arbeidet ikke å gjøre noen realitetsendringer ved omfanget av straffelovens § 145. Det sentrale var å få klargjort at regelen også var anvendelig på ”(...) informasjon som er lagret på eller overføres ved hjelp av EDB eller andre tekniske midler.”¹⁵ Den raske teknologiske utviklingen i samfunnet, hadde medført at en modernisering av språket i § 145 var blitt nødvendig. Dessuten var en bedre presisering av lovens rekkevidde ønskelig. Denne presiseringen ble gjennomført ved å legge til et nytt annet ledd i § 145. I innledningen av første kapittel i Ot.prp.nr.35 1986-1987 sies det; ”Strl. § 145 om brevbrudd foreslås gitt et tillegg slik at det får klarere fram at den også rammer det å skaffe seg uberettiget adgang til data.”.

¹³ Ot.prp.nr.4 (1978-1979). Om lov om endringer i straffeloven side 6 flg.

¹⁴ NOU 1985:31 - Datakriminalitet

¹⁵ Ot.prp.nr.35 1986-1987 side 20.

Det foregår i dag et arbeid med å finne nye måter å bekjempe datakriminalitet. Den 8.11.2001 fikk man Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi. Norge undertegnet konvensjonen 23.11.2001. Kort tid etter, 11.01.2002, opprettet man så datakrimutvalget. Formålet med dette utvalget er å utrede de eventuelle lovendringer som må til for at norsk lov ikke skal bli konvensjonsstridig. 4. november 2003 ble utredningen overlevert til Justis- og politidepartementet, i form av NOU 2003:27.

Videre fikk man også et høringsutkast om forslag til endringer i åndsverksloven. Dette er utgitt av kultur- og kirkedepartementet, med høringsfrist 25. juni 2003. Dette har riktignok ikke en direkte sammenheng med straffelovens § 145, men eventuelle endringer i åndsverkslovens § 12 om rett til privat eksemplarframstilling, kan få konsekvenser for eksempel for om adgangen til et verk er ”uberettiget” eller ikke. Resultatet av høringsutkastet ble Ot.prp.nr.46 (2004-2005) - Om lov om endringer i åndsverkloven m.m. Nytt her er at det er innført begrensninger i retten til privateksemplarstilling etter åndsverksloven § 12, hvis det blir foretatt en omgåelse av ”tekniske beskyttelsessystemer”. Disse begrensningene i åndsverksloven § 12 kommer som en følge av at man ønsker å implementere Infosoc-direktivets artikkel 6.

2.2 *Hva er omfattet av ”data” i lovens forstand?*

For at den tiltalte gjerning skal kunne bli omfattet av straffelovens § 145 annet ledd, må handlingen innebære å ”(...) bryte en beskyttelse eller på lignende måte uberettiget skaffer seg adgang til data(...) som er lagret(...)”¹⁶. Et viktig spørsmål blir da om man kan si at den tiltalte faktisk har skaffet seg adgang til ”data”. I DVD-dommens tilfellet, blir da spørsmålet om en film er å anse som ”data”. I denne sammenheng, så har Høyesterett tidligere avsagt to dommer hvor det har blitt uttalt at fjernsynssendinger faller utenfor databegrepet i § 145 annet ledd. Disse dommene har et noe annet faktum,

¹⁶ Straffelovens § 145 annet ledd.

men Høyesteretts tolkning av rekkevidden av databegrepet vil allikevel kunne være av interesse. Jeg vil behandle disse dommene for seg selv under kapittel 2.3.

Lagmannsretten slår i DVD-dommen raskt fast at man her har med et tilfelle som faller innenfor begrepet ”data”, med følgende setning.

”Spørsmålet blir først hva som ligger i uttrykket « data ». Lagmannsretten legger til grunn at i denne saken må uttrykket omfatte både filmen og Content Scrambling System programmet. Forstått slik kan det ikke være tvilsomt at saken omhandler « data » i lovens forstand.”¹⁷

Det er litt overraskende at dette bare blir lagt til grunn i en setning, uten en videre drøftelse, spesielt da med tanke på de to nevnte avgjørelsene fra Høyesterett. Det er også flere spørsmål som trer frem. For det første kan det spørres om det faktisk er slik retten sier, at filmen og CSS skal ses under ett, med tanke på avgjørelsen om vi står ovenfor data eller ikke, i lovens forstand. For det andre er det et spørsmål om hva databegrepet i lovens forstand faktisk innebefatter. Er for eksempel en film ”data” i lovens forstand? Videre, er CSS ”data” i lovens forstand? Et annet spørsmål er om CSS, eventuelt en annen sikkerhetsanordning, vil kunne være data, når den er implementert får å beskytte noe annet. Dette er spørsmål som retten lar ligge, uten en videre drøftelse, som kanskje burde vært grundigere belyst.

2.2.1 Hva er ”data”?

Jeg vil her i første omgang se om en film vil kunne være omfattet av databegrepet, for så å se på rekkevidden av databegrepet mer generelt.

Straffelovens § 145 første ledd rammer som;

¹⁷Se vedlagt kopi av DVD-dommen, avsnitt 18.

”(...)uberettiget bryter brev eller annet lukket skrift eller på liknende måte skaffer seg adgang til innholdet, eller baner seg adgang til en annens låste gjemmer(...)”.

Som nevnt over, så ble annet ledd tilføyd, for å klargjøre at regelen også omfattet data som ble lagret eller overført elektronisk. Annet ledd er således en utvidelse av den originale brevbruddsbestemmelsen. Den ble innført for å bedre takle nyere teknologi, men det kan tas til orde for at hva som beskyttes fortsatt er det samme. Hvis man ser på første ledd isolert sett, så vil man se at det ikke er utslagsgivende hva brevet eller ”(...)låste gjemmer(...)” måtte inneholde. Det utslagsgivende vil være adgangen er ”uberettiget”, og at man har brutt et brev eller et lukket skrift, eller på en ”lignende måte” har skaffet seg adgang til innholdet. Hva innholdet måtte være er ikke av betydning. Dette vil kunne tale for en vid tolkning av databegrepet, etter som det som man ønsker å beskytte, første og annet ledd, vil være sammenfallende. For eksempel ville første ledd kunne omfatte et brev som innholdt en film. Dette ble det også tatt til orde for i forarbeidene til endringene i 1979, hvor det ble uttalt; ” (...)lydbånd i lukket omslag bør ha samme beskyttelse som skriftlige opptegnelser.”¹⁸ Man kan således på dette grunnlag kunne ta til orde for at regelen i annet ledd også skal kunne omfatte lyd, bilde og, når de ville blitt beskyttet i første ledd. Ved endringene i straffelovens § 145 i 1987¹⁹ ønsket man jo, som nevnt innledningsvis, å få klart meddelt at lagring og overføring av ”data” ved hjelp informasjonsteknologi også var omfattet av paragrafen. Det var ikke ment at lovendringene skulle gi § 145 noe snevrere innhold enn det den tidligere hadde. Det kan således tas til orde for at det som får vern av første ledd også vil bli vernet av annet ledd, så langt de øvrige vilkårene er oppfylt.

I NOU 1985:31 (Datakriminalitet) s 32 annet avsnitt, bruker man eksempelet om at en meddelelse som er lest inn på plate eller lydbånd vil være omfattet av § 145 annet ledd. Som nevnt over så har man også i forarbeidene fra 1979 uttalt at lydbånd i lukket omslag ville være omfattet etter første ledd.²⁰ Dette var da før innføringen av annet ledd.

¹⁸ Ot.prp.nr.4 (1978-1979) Om lov om endringer i straffeloven, side 9.

¹⁹ Ot.prp.nr.35 1986-1987, side 5, femte avsnitt.

²⁰ Ot.prp.nr.4 (1978-1979) Om lov om endringer i straffeloven, side 9.

Dette vil medføre at lyd på lydbånd, telefonsvarere, mobiltelefoner med mer vil også være ”data”

Man må også kunne tolke endringene av § 145 i 1987 i lys av at de ble gjort for å bedre kunne takle det økende problemet med datakriminalitet²¹. Man ønsket heller ikke her å foreta en realitetsendring av regelen, noe som skulle tale for at innføringen av ordet ”data”, i annet ledd ikke skulle forandre regelens omfang. I forarbeidene²² til endringene i 1987 uttales det at;

”§145 annet ledd vil også ramme det å skaffe seg adgang til innholdet av telegram, telex, telefax og liknende telekommunikasjonsmessige overføringer, jf forarbeidene til det tidligere §145 annet punktum tilføyd i 1979 (Ot prp nr 4 (1978-79) s 9).”

Vi kan se her at telefaks er positivt nevnt i forarbeidene. Når en telefaks blir brukt vil den overføre et bilde av dokumentet. Dokumentet blir kodet og oversendt til en annen faksmaskin. Faksen kan således fint brukes til å oversende fotografier og tekst, håndskrift eller ikke. Telefaksen vil behandle alt den overfører likt. Det som blir overført blir gjort om til et bilde. Mottaker maskinen vil så motta koden, lage et bilde av koden, for så å skrive det ut. Man har således i forarbeidene, sagt at overføring av bilder er omfattet av regelen, og i så måte faller også bilder inn under definisjonen av ”data”. Bilder er jo i seg selv et vidt begrep, og vil omfatte skisser, tegninger, malerier og fotografier.

Hvis man ser for seg en film, så er den sammensatt av to elementer, bilder og lyd. Riktig nok er det snakk om bilder i bevegelse, men denne bevegelsen oppstår som følge av at det vises mange enkeltbilder i rask rekkefølge. Når disse to elementene, lyd og bilde, hver for seg er omfattet av databegrepet, så taler mye for at når man slår de to delene sammen til en film, at også denne burde være omfattet.

²¹ Datakriminalitet er der hvor utnyttning av datateknologi har vært vesentlig for overtredelsen.

²² Ot.prp.nr.35 1986-1987 side 21.

Man må således kunne si, som lagmannsretten gjør i DVD-dommen, at en film er omfattet av databegrepet.

Annet ledd omfatter i tillegg til ”data”, også ”programutrustning”. Her har lovgiver ikke vært konsekvent i sitt ordvalg i forhold til annen lovgivning. Forarbeidene²³ sier at ”(...)også « programutrustning », dvs instruksjonene til maskinen (dataprogrammer) (...)” er omfattet. Bakgrunnen for at man bruker denne formuleringen er at man ønsket å bruke samme formulering som i straffelovens § 270 første ledd nr. 2. I åndsverksloven bruker man formuleringen, datamaskinprogrammer, blant annet i § 39g. En forklaring kunne ha være at lovgiver mente at databegrepet ikke omfattet dataprogrammer, og la derfor til, programutrustning.

Det heter i rettskildelæren at man skal, så langt det er mulig, tolke loven gjennom bruk av en normal språkforståelse. Hva man så forstår med ordet ”data”, etter en normal språkforståelse, vil da være av stor betydning for rekkevidden av § 145 annet ledd. Med dette menes hvordan man i dagligtalen ville forstå ord og uttrykk, og legge dette til grunn for lovtokningen. Dette er allikevel ikke alltid like lett å gjennomføre i praksis. Dette spesielt når loven opererer innenfor spesielle fagfelt, hvor man kan ha en egne forståelse av ord og uttrykk. I slike tilfeller må man bruke det utvidede begrepsabaratet fra de spesielle fagfeltene. Slike spesialiserte betegnelser kan ofte bli brukt i dagligtalen, men da uten de samme nyansene som man ville operere med i fagfeltet. Ordet ”data” faller kanskje litt inn under det sist nevnte, uten å egentlig å tilhøre et spesielt fagfelt, men blir nok brukt av flere, og kan bli tillagt forskjellig definisjon innenfor hvert enkelt felt.

Hvis man ser hvordan ordet ”data” blir brukt i dagligtalen, vil man nok ofte se at tankene går til områder rundt datamaskiner og dataprogrammer. I informatikken vil man operere med tre skiller, ”tegn”, ”data” og ”informasjon”. Nederst vil man finne ”tegn”, som for eksempel bare vil være et tall, en bokstav eller komma. I seg selv vil ikke dette være nok til å bli ansett som data. Når tegn blir satt i en eller annen form for

²³ Ot.prp.nr.35 (1986-1987) Om endringer i straffeloven (datakriminalitet) side 20 annet avsnitt.

sammenheng, vil man kunne få ”data”. Tegnene vil da være med på å beskrive et eller annet, og kan så bli ansett som ”data”. Når ”data” igjen blir tolket vil man kunne ende opp med ”informasjon”.

Alternativt, i dagligtalen, vil man nok få assosiasjoner til informasjon eller opplysninger, da gjerne igjen brukt som synonymmer til hverandre. Dette er nok heller ikke fullgode synonymmer med ”data”. ”Data” inneholder definitivt mer enn bare dataprogrammer, og informasjon inneholder nok også noe mer enn bare ”data”. Det kanskje mest passende synonymet til ”data”, vil kanskje være, opplysninger, men selv dette er nok ikke helt dekkende. Man kan kanskje si at informasjon får man først når man setter ”data” i en subjektiv sammenheng eller etter en subjektiv fortolkning av dataene. Eller som sagt av Selmer;

”Informasjon kan ikke lagres eller overføres. Informasjon oppstår først i et menneskets (eller dyrs) bevissthet når dette noe som er ”data” blir sett, hørt, følt eller på noen måte brakt innenfor rekkevidde av sanseapparatet.”²⁴

Informasjon blir således en mer subjektiv tolkning av ”data”. Den samme dataen kan da gi forskjellig informasjon til forskjellige mennesker. I sin doktoravhandling foretar Bing også et lignende skille, og utaler;

”(…) sonderer jeg altså mellom « data » og « informasjon ». For at data skal transformeres til informasjon, må data komme frem til noen som kan bruke dem, og denne noen må ha midler til å kunne forstå dataene.”²⁵

Man kan ut i fra dette se at hvis man for eksempel kommer over et tekstdokument som er krypterte, og man av den grunn ikke kan lese det. Man vil således ikke ha mottatt noe informasjon, men man vil allikevel ha mottatt data.

Selmer tar også til orde for en vid fortolkning av ”data”.

²⁴ Fra artikkelen ”Hva er ’data’?” av Knut Selmer i Lov & Data 1995-042.

²⁵ Bing, Jon - Rettslige kommunikasjonsprosesser side 67.

”’Data’ kan være bokstaver, streker og farger i et bilde, fakter, lyd, lys, elektromagnetiske impulser, spor i et elektronisk lagringsmedium. Data er alt som – dersom man bare har de riktige innretninger for å skape sanseinntrykk kan føre til at et levende vesen får en bestemt, tilsiktet informasjon”.²⁶

Med en så vid tolkning kan det spørres om det er mulig å overføre eller lagre noe, digital eller analogt, som ikke er å anse som ”data”. Det kan spørres om det lar seg gjøre å sette en klar grense for hvor vidt databegrepet kan tolkes. ”Data” må ikke forveksles med maskinlesbare opplysninger. De kan være sammenfallende, men ikke fordi dataene er maskinlesbare eller fordi de er formidlet med informasjonsteknologi. Opplysninger i et dokument blir ikke mer ”data” hvis det er lagret på en diskett enn hvis de er skrevet ut på et ark. Nå er det nok slik at i praksis, så vil nok de aller fleste tilfeller som er omfattet av straffelovens § 145 annet ledd, vil være data som er lagret digitalt. Men det må nødvendig hvis ikke være tilfellet. En overføring av data over en analog telefaks, vil klart falle innenfor § 145. De fleste telefakser overfører fortsatt data analogt over telefonlinjer.

I forarbeidene til endringen av 1987 uttales det: ” Uttrykket «data» omfatter all slags informasjon, f eks om personlige, tekniske eller økonomiske forhold. Begrepet må forstås vidt.”²⁷ Man får her litt innblikk i hva man ønsker at databegrepet skal inneholde, og at det skal foreligge en vid fortolkning. Samtidig så ser vi at man bruker ordet informasjon som et synonym til ”data”, noe som vi har sett over at det ikke er.

2.2.2 Nedre grense for databegrepet.

Det å gi en god avgrensning av ”data” er ikke lett. I forarbeidene²⁸ til endringene i 1985 utales det at avgrensningen av ”data” får man gjennom lovens vilkår om ”(...)som er

²⁶ Fra artikkelen ”Hva er ’data’?” av Knut Selmer i Lov & Data 1995-042.

²⁷ Ot.prp.nr 35 1986-1987 (datakriminalitet) side 20 annet avsnitt.

²⁸ NOU 1985:31 Datakriminalitet – side 31 annet avsnitt.

lagret eller overføres ved elektroniske eller andre tekniske midler.”. Man sier her at man har funnet det vanskelig å finne en eksakt avgrensing av ”data”, men at så lenge det blir lagret eller oversendt elektronisk, så vil det være omfattet. Dette taler for et meget vidt begrep.

Et tenkt tilfelle ville være en person som prøver å bryte seg inn på et nettverksområde hvor han ikke har tilgang. Hvis det så viser seg at dette området ikke inneholder noe ”data”, vil det fortsatt være omfattet av § 145 annet ledd? Det kan ved første øyekast se ut til at ingen skade har skjedd, og ingen data kom på avveie. Lovtekstens ordlyden kan også tyde på at det bør være *noe* som er lagret eller overført for at regelen skal kunne komme til anvendelse. På en annen side, vil et område hvor det ikke finnes data, også kunne gi informasjon om noe annet. Denne informasjonen burde kanskje ha rett til å bli vernet på lik linje med informasjon som bygger på tilstedeværelsen av ”data”. Et eksempel kan være å bryte seg inn i safen hvor man vet at ens tante oppbevarer sitt testamente. Hvis safen så viser seg å være tom, vil dette kunne fortelle mye om et fremtidig arveoppgjør, og således inneholde informasjon.

Hvis man trekker dette videre og sier man kun finner tekstdokumenter med kun en masse vilkårlige tegn, så vil dette gi kunne like lite mening som et tomt dokument, og burde kunne likestilles med det. Et annet eksempel vil være en finner en opptegning av alfabetet. Dette vil nok heller ikke være en bærer av noen beskyttelsesverdig data. På den annen side, hvis man i mitt eksempel over om testamentet, fant et dokument i safen, hvorpå det var skrevet alfabetet flere ganger. Resultatet vil også være her at man sitter igjen med informasjon. Ikke som følge av det man fant, men som en følge av hva man ikke fant, sett sammen med den forkunnskapen eller forventningene man hadde til den dataen som skulle ligge i safen.

Et annet eksempel vil kunne være om man bryter en beskyttelse for så å få tilgang til et tom Word-dokument. Dette vil inneholde data om for eksempel når dokumentet ble laget, av hvem, når det sist ble redigert samt en data om formatering med mer. Det kan spørres om dette tilstrekkelig for å bli omfattet av ”data” i § 145 annet ledd.

Disse eksemplene leder oss til å spørre om databegrepet bør begrenses til å kun omfatte ”data” som bærer av potensiell informasjon. Dataen må altså kunne tolkes, og gi informasjon. Dette ville da blant annet medføre at en oppramsing av alfabetet, som ikke er en bærer av nevneverdig informasjon, ikke ville bli å anse som ”data” i § 145 annet ledds forstand.

Man må da få avklart for hvem dataen skal kunne gi potensiell informasjon. Den tiltaltes forkunnskaper vil nok ikke være avgjørende for om man står ovenfor ”data” eller ikke. Dette kan vises ved tilfellet hvor man bryter seg inn og finner et kryptert dokument. Hvis den tiltalte ikke har nøkkelen til dokumentet, og ikke har andre måter å bryte det opp på, så vil dette dokumentet fortsatt være ”data”, selv om den tiltalte ikke klarer å utlede noe informasjon av det. Hvis jeg mottar et brev på et språk jeg ikke forstår, så vil ikke dette gi meg noe informasjon, men det vil fortsatt være ”data”.

”Data” bør således objektivt sett være en bærer av potensiell informasjon. Et annet eksempel som taler for en slik fortolkning får man hvis to personer bryter seg inn i det samme området. Uavhengig av deres forkunnskaper eller forventinger til hvilken informasjon de skal kunne utrede, bør de bli behandlet likt, selv kun en av de klarer å tyde dataene.

Fra lagmannsretten i NDD-dommen utales det;

”Endelig presiseres at det ikke er en forutsetning for anvendelsen av bestemmelsen at gjerningsmannen har gjort seg kjent med innholdet i informasjonen.”²⁹

Dette taler også for at man ikke ser på den tiltaltes mulighet til å fortolke dataene, da § 145 annet ledd vil kunne komme til anvendelse selv om man ikke har gjort seg kjent med innholdet.

²⁹ LB-1997-1527 (Lovdata har dessverre ikke lagt til sidetall, men kommentaren finnes på side 5 av en utskrift av lovdata).

Ved å si at man ikke legger vekt på den tiltaltes forkunnskaper, sier man også at eksemplene over om å bryte seg inn i et tomt område, ikke vil kunne være å anse som ”data” i lovens forstand. Det er en uønsket handlig, men man skaffer seg ikke tilgang til ”data”. Man kan ikke legge gjerningsmannens forhåpninger til hva han skulle finne, grunn for avgjørelsen om man står ovenfor ”data”. I praksis vil dette heller la seg gjennomføre, da man ikke kan vite hva gjerningsmannen håpet å oppnå med innbruddet.

2.2.3 Kan beskyttelsen (CSS) være data?

CSS er som nevnt det datamaskinprogrammet som er brukt på de fleste DVD filmer, til å fremstille en kryptert versjon av filmen. Etter at programmet er kjørt vil filmen således ikke være leselig uten en nøkkel. CSS fyller således en funksjon som både kopibeskyttelse og avspillingsbeskyttelse. Det er altså denne beskyttelsen den tiltalte var tiltalt for å ha omgått, for å ha skaffet seg adgang til filmen.

Jeg tar her utgangspunkt i følgende uttalelse i DVD-dommen.

”Spørsmålet blir først hva som ligger i uttrykket ”data”. Lagmannsretten legger til grunn at i denne saken må uttrykket omfatte både filmen og Content Scrambling System-programmet. Forstått slik kan det ikke være tvilsomt at saken omhandler ”data i lovens forstand.”³⁰

Det oppstår her to spørsmål. For det første, om man i avgjørelsen om man står ovenfor ”data” i lovens forstand, kunne se på beskyttelsen (som CSS) og det som skal beskyttes, under ett. For det andre, om beskyttelsen på selvstendig grunnlag kan være både ”data” og beskyttelse.

Selve CSS-programmet finnes dog ikke på DVD-platen. Men på platen ligger det koder som tilhører CSS. Over har vi sett at databegrepet må fortolkes meget vidt. Nøkklene og

³⁰ DVD-dommen avsnitt 18 i vedlagt kopi.

kode som CSS-programmet har lagt på DVD-platen vil således være å anse som ”data”.

Når det gjelder det første spørsmålet, så vil det i DVD-dommens tilfellet være mest naturlige å se filmen som den ”dataen” som skal beskyttes i § 145 annet ledd. CSS vil da være den beskyttelsen som måtte brytes for å få adgang til dataene. En analogi til et innbrudd, kan være med på å belyse situasjonen. Den låsen vil da være beskyttelsen til huset, som da vil være dataen. Det vil her føre galt av sted hvis man skulle slå sammen låsen og huset, til en ting. Låsen er der for å hindre uvedkommende adgang til huset. Man ville i så fall kunne ende opp med en situasjon hvor man sier at tyven også har brutt seg inn i låsen, til det huset han har brutt seg inn i. Jeg kan vanskelig se at en slik sammenslåing vil være hensiktsmessig.

Det er jo også en grunn til at man har to vilkår, om ”beskyttelse” og ”data”. Hvis beskyttelsen også var ”data”, hadde det strengt talt ikke vært nødvendig med et vilkår om ”data”. Et hvert brudd på en beskyttelse ville da ha vært omfattet.

Videre kan man komme i den situasjon hvor man har lagret noe som ikke er å anse som ”data”, og der med heller ikke omfattet av § 145 annet, og dette allikevel vil bli omfattet fordi man har implementert en beskyttelse rundt det. Et eksempel ville være at man har lagret et dokument som inneholder alfabetet, som nok ikke er å anse som data. Dette ville da allikevel bli omfattet hvis man har en beskyttelse rundt dokumentet. Det samme ville være om man satte opp en beskyttelse rundt et tomt område. Å gi beskyttelsen en slik utvidende effekt av databegrepet var nok eller ikke lovgivers intensjon.

Beskyttelsen er der for å hindre uvedkommendes innsyn til ”data”. Hvis man åpnet for muligheten for at man skulle kunne ta med beskyttelsen i vurderingen om man står ovenfor ”data”, vil man kunne ende opp med å gi § 145 annet ledd en endeløs rekkevidde, så lenge man har en beskyttelse.

Et annet spørsmål blir så hva følgene blir av om man legger en beskyttelse utenpå en annen beskyttelsen. Tanken her ville være at man ønsket å få beskyttelsessystemet sitt til å bli beskyttet av § 145 annet ledd. Dette blir litt som å legge en lås på en lås. Det at

man må bryte opp en lås får å få tilgang til låsen på døra, gjør ikke at har foretatt ett innbrudd når man får tilgang til den innerste låsen. Det at man velger å implementere to beskyttelsessystemer, vil ikke gjøre noe annet enn at man har litt mer sikkerhet. Beskyttelsessystemet kan defineres ved at de er til for å beskytte dataene. Det at det er flere lag av de, forandrer ikke deres karakter. Lovteknisk er det også nødvendig å trekke en sontring mellom ”data” og ”beskyttelsen”. Dette så de oppfyller kun en funksjon i lovteksten.

2.3 Dekoderdommene.

Som nevnt innledningsvis, så har høyesterett ved to tidligere anledninger tatt stilling til innholde av databegrepet i § 145 annet ledd. Disse kan være med på å belyse databegrepets omfang i lovens forstand. Saken som er oppe til avgjørelse skiller seg noe fra DVD-dommen. Man ønsker å se om fjernsynssendinger er å anse som ”data” i lovens forstand. Som nevnt over, så ble ikke disse dommene nevnt av lagmannsretten, når den kommenterte databegrepet. I begge de to nevnte dommene uttalte Høyesterett at databegrepet i § 145 annet ledd ikke omfatter fjernsynssendinger. Dommene det her er snakk om er, Rt-1994-1610 og Rt-1995-10, heretter omtalt som dekode dommen I og II. Dekode dommen II behandler dog ikke temaet ut over å vise til resultatet i den første, og sier seg enig med resultatet.

I begge de nevnte sakene hadde de tiltalte blant annet, produsert og solgt såkalte piratsmarkkort for fjernsynsdekodere. Bruk av disse ”piratsmarkkortene”, og gav brukeren en urettmessig tilgang til betalingskanaler, ved at man ikke trengte å betale for tjenesten. Betalingskanaler ble distribuert sammen med de andre kanalene, man sendte de ut over kabel-tv, til alle som hadde kabel-tv. Også til de som ikke ønsket å benytte seg av betalingskanalene. Kabel-tv selskapet la så til støy på disse sendingene. Hvis man så prøvde å se på betalingskanalen ville man i beste fall få dårlig bilde- og lyd kvalitet. Det mest vanlige var dog at man kun fikk vist støy på fjernsynet, og ikke noe som man kunne se på. Ønsket man å se på kanalen måtte man betale. Man fikk da tilsendt et markkort, som man puttet i dekode ren. Dette kortet ga dekode ren mulighet til

å fjerne støyet som lå på sendingene til betalingskanalene, og man fikk så et klart bilde. De tiltalte i hadde laget smartkort som fungerte på den samme måte.

Dekoderdommen II går ikke inn og diskuterer saken, ut over å referere til den første. Den vil allikevel få en rettskildemessig relevans, da den er med på å bekrefte Høyesteretts standpunkt fra den første saken.

Rettskildemessig, så er utgangspunktet i Norge at retten ikke bundet av tidligere avgjørelser. Det vil si at retten kan velge et annet resultat ved en senere anledning. Dette er dog kun i teorien, i praksis står prejudikatslæren sterkt. Man pleier å si at alle domstoler, da naturlig nok med unntak av Høyesterett, er bundet av en avgjørelse avsagt av en domstol av en høyere rang. En tingrett vil altså ikke uten videre kunne gå imot en tidligere avsagt lagmannsrettsdom. Den eneste domstolen som vil gå i mot en Høyesterettsavgjørelse, vil da være Høyesterett selv. Det er også antatt at dommer fra Høyesterett i plenum, står sterkest.

Det finnes eksempler på at et spørsmål har kommet opp for Høyesterett, hvor saken har blitt avgjort ved dissens. Så har en sak med det samme saksforhold kommet opp for Høyesterett kun et par dager senere, avsagt av de samme dommerne. Her vil man da se at dommerne tar den tidligere avsatte dom til etterretning, og stemmer for det samme resultat i den nye dommen, men nå enstemmig. Vi kan her se et eksempel på at Høyesterett følger en tidligere avgjørelse, og lar denne få utslag i den nyere dommen, og viser at det ikke lenger er tvilsomt for retten hva rettstilstanden er. Dette er også hva som var tilfellet ved de to nevnte dekode dommene. Den første ble avgitt med dissens, og den siste ble avgitt enstemmig.

Det er allikevel skjedd, at Høyesterett har forandret oppfattning på et område. Når dette skjer og det ikke følger av at det er foretatt endringer i loven, så er gjerne den omgåtte dom gammel, tiden har gått fra den. Eventuelt at det skjer en gradvis endring av praksis. Da gjerne i tilfeller hvor loven viser til uttrykk av moralsk karakter. Eksempler på slike

uttrykk vil kunne være ”utilbørlig” eller ”ærbarhet”.³¹ Man kan så ilegge disse uttrykkene nye verdier, og rettspraksis kan gradvis endres. Når er dekodeordommene av en ganske ny dato, så man kan vanskelig bare si at tiden har gått fra disse dommene.

En annen fremgangsmåte som man har sett Høyesterett bruke, når den ønsker å gå imot en eldre dom, er å differensiere i faktum. Man vil da si at faktum for de to tilfellene, den eldre dommen og den man avsier, er så forskjellige at man ikke kan bruke den eldre dommen som presedens på faktumet i den nye dommen. Det er mulig at lagmannsretten har ment at dette var tilfellet med DVD-dommen opp mot dekodeordommene, og at det er derfor dekodeordommene ikke er nevnt. Dette da med utgangspunkt i lagmannsrettens uttalelser om at filmen og krypteringsprogrammet, CSS, sammen utgjør ”data” i lovens forstand. Det kan være at retten her ønsket å differensiere faktum i denne saken fra den i de tidligere høyesterettsdommene ved å si at dette er forskjellig fra en fjernsynsringkasting.

2.3.1 Dekoder dommenes tolkning av ”data”.

I dekodeordommen I går Høyesterett gjennom noe av historikken bak § 145. Hvorpå første voterende sier:

”Jeg bemerker at selv om man her omhandler telekommunikasjonsmessig overføring av stoff, viser eksemplene at man ikke har hatt fjernsynssignaler eller fjernsynsprogrammer i tankene. Bemerkningene til forslaget fra Straffelovrådet, som er sitert i proposisjonen, var også knyttet til lydbånd, teleks og opplysninger i dataanlegg.”³²

Dette viser at faktum skiller seg noe fra faktum i DVD-dommen, hvor det ikke var snakk om noen ringkasting. At det er forskjeller i hvordan en film eller et fjernsynsprogram blir formidlet er i utgangspunktet ikke avgjørende. Straffelovens

³¹ Se Eckhoff– Rettskildelære, utg. 4 kap 7, VII

³² Rt-1994-1610 side 1612 fjerde avsnitt.

§ 145 omfatter ”data” som er lagret og som sendes over datanettverk, teleks, telefon, med mer. Veien er således ikke lang å gå for at § 145 også skal kunne omfatte overføring av fjernsynssignaler. Dette kan vi blant annet se ved at mange i dag har tilgang til internett gjennom den samme kabelen de mottar sitt fjernsynssignal. Samtidig kan vi se at trådløse nettverk blir mer og mer vanlig. Vi kan også se at i forarbeidene til endringen i straffeloven i 1987, så var det fremmet et forslag om å la en ny § 403 i straffeloven omfatte det å tilsnike seg bruk av fjernsyn.³³ Det ble også uttalt at § 145 omfattet;

”(...)datalogrede opplysninger er tilgjengelig for allmennheten mot erleggelse av betaling, og at den innlagte sperre bare har som formål å sikre betaling blir ytet.”³⁴

Justiskomiteen fjernet senere forslaget om ny § 403 under henvisning til at en krenkelse av betalingsinteressen var rammet av § 145 annet ledd.³⁵ Denne argumentasjonen ble også støttet av mindretallet i dekoderdommen I.

Førtevoterende deler ikke dette synet og uttaler;

”Rent språklig ligger det nærmest å forstå uttrykket data slik at det omfatter faktiske opplysninger og informasjon. Det er ikke naturlig å forstå det slik at det omfatter fjernsynsprogrammer. Jeg kan videre ikke se at forarbeidene gir grunnlag for noen utvidende fortolkning.”³⁶

og,

³³ Ot.prp.nr.35 (1986-1987) side 16.

³⁴ NOU 1985:31 side 31 høyre spalte tredje avsnitt.

³⁵ Ot.prp.nr.35 (1986-1987) side 21 nest siste avsnitt.

³⁶ Rt-1994-1610 side 1612, 11 avsnitt.

”Men som jeg tidligere har nevnt, finner jeg det ikke naturlig å forstå uttrykket data slik det er brukt i sammenhengen i § 145 dit hen at det også omfatter fjernsynsprogrammer.”³⁷

Den første uttalelsen er litt merkelig, da det i proposisjonen faktisk blir nevnt at man ønsker en vid forståelse av uttrykket data.

Det skal sies at den første dommen ble avsakt med sterk dissens, tre mot to. Mindretallet uttaler blant annet:

”Jeg ser det slik at fjernsynssignalene – og derved fjernsynsprogrammene – fra betalingsfjernsyn som TV 1000 naturlig må forstås som data som er beskyttet mot innsyn fra uberettigete.”.

Selmer har uttalt at han ikke deler syn med Høyesterett, og begrunner blant annet sitt syn på denne uttalelsen.³⁸ Det er dog verdt å merke seg at denne uttalelsen kommer fra mindretallet i dommen.

I 1994 var fortsatt fjernsynssendinger i all hovedsak analoge. Det kan således reises et spørsmål om sakens utfall ville blitt annerledes hvis det hadde vært snakk om digitale sendinger. Høyesterett nevner ikke problemstillingen, og gjør ikke et poeng ut av at kodingen av sendingene gjøres ved at det legges til støy i sendingen, som så kan fjernes av dekoderen. Begrunnelsen ligger i all hovedsak i at det er snakk om en fjernsynssending. Det om den er analog eller digital burde således ikke ha en nevneverdig betydning. Det er lite eller ingenting som taler for at en digital sending fortjener et bedre rettslig vern enn en analog.

På tidspunktet for denne avgjørelsen forelå det forarbeider til en ny § 262 i straffeloven, i form av Ot.prp.nr.4 (1994-1995). Om lov om endringer i straffeloven m.m. Denne omfattet salg og markedsføring av slike piratsmarkert som dekodedommen

³⁷ RT-1994-1610 side 1613 femte avsnitt annen setning.

³⁸ Se artikkelen ”Hva er data?”

omhandler. Det kommer også frem at departementet mente at dette tilfellet er omfattet av § 145 annet ledd, men av lovtekniske grunner ønsker man å plassere denne regelen under kapittel 24 om underslag, tjueri og ulovlig bruk, i straffelovnen. Både flertall og mindretall har kommentert dette, hvor det blant annet uttales:

”De signaler som overføres ved en fjernsynssending, må anses for å være data i lovens forstand. (...) Overføring av fjernsynssignaler er en form for telekommunikasjonsmessig overføring.”³⁹

Mindretallet mener at dette bygger opp under deres forståelse av § 145, og ser på den nye § 262 som en *lex spesilalis*, som ikke vil innskrenke rekkevidden av § 145.⁴⁰ Flertallet i dekoderdommen I viser også til proposisjonen, og sier at man ikke deler departementets syn på tolkningen av § 145. Førstvoterende uttaler,

”Av proposisjonen fremgår at bestemmelsen er ment som en klargjøring, idet det er antatt at det allerede følger av gjeldende rett at det er straffbart å markedsføre privatdekodere. Det er blant annet vist til herredsrettens dom i vår sak. Som jeg allerede har gitt uttrykk for, deler jeg ikke dette syn.”⁴¹

Høyesterettsdommene viser uansett at det finnes en avgrensning av databegrepet, mot fjernsynssendinger. Det ser ut til at øvrig juridisk litteratur ikke er villig til å akseptere høyesteretts forståelse av data i de to dekoderdommene. Rettskildemessig er dette ganske unikt. Normalt vil en avgjørelse av Høyesterett være et meget tungtveiende argument. Hvis det i tillegg kommer flere dommer i samme retning, så vil man si at rettstilstanden er avklart. I dette tilfellet dog, så er det vel kun Schjølberg som ser ut til å holde seg Høyesteretts fortolkning. Han har uttalt at, uansett hvordan man tolker ”data”, så er det ikke naturlig å forstå § 145 annet ledd slik, at lyd og bilder omfattes. Videre

³⁹ Ot.prp.nr.4 (1994-1995). Om lov om endringer i straffeloven m.m. side 50 syvende avsnitt.

⁴⁰ Dekoderdommen I side 1616 tredje avsnitt.

⁴¹ Dekoderdommen I side 1613 siste avsnitt.

sier han; ”Det er utvilsomt at rammen for bestemmelsen er datamaskiner, datasystemer eller nettverk hvor representert vanlig skriftlig eller tekstlig informasjon”⁴²

2.3.2 Dekoderdommenes rekkevidde.

Jeg synes at rettens resultat her er problematisk, spesielt med tanke på den raske teknologiske utviklingen. Man har i den seneste tiden sett en sammensmelting av flere typer media. Det som før var atskilt og forskjellig ting med forskjellige egenskaper blir nå en ting. Mest synlige ting på dette er for eksempel at kompaktplatespiller og video spiller/opptager blir ett. Det samme med fjernsyn og datamaskin. Snart vil vi nok også se at alle disse egenskapene blir inkorporert i en boks, og vi sitter kun igjen med en datamaskin. Det vil da bli vanskelig å skille et fjernsyn fra en datamaskin. Dette særlig for den vanlige sluttbrukeren. Et eksempel på dette vil være innføring av digitalt kabel-tv med såkalt ”Pay per view”. I dag er dette en ordning hvor man for eksempel har en informasjonskanal med en oversikt over en rekke filmer og andre fjernsynsprogrammer. Hvis man ser noe av interesse, så kan man velge å betale for å få tilgang til kanalen hvor programmet går. Dette vil nok være med på å strekke det daglige begrepet av fjernsyn. På data siden, så har man såkalt ”Streaming”⁴³ av video over internettet. Dette er en internett tjeneste som kan gjøres tilgjengelig mot betaling. Her vil man få tilgang til et nett område hvor man vil motta en kontinuerlig datastrøm i form av video og/eller lyd. Denne dataen blir i utgangspunktet ikke lagret på datamaskinen, men avspilt umiddelbart. I dag er det ganske greit å skille disse to tjenestene, da de leveres for to fysisk forskjellige maskiner. I den nærmeste fremtid, så vil vi nok se en sammensmeltning av fjernsynet og datamaskinen. Når de to tingene blir en, så vil det bli vanskelig for brukeren å se noen forskjell på de to tjenestene som blir levert. Det kan da spørres om det er hensiktsmessig i et slikt tilfelle, å skille fjernsynssendinger fra data.

Dommens rekkevidde må nok kunne sies å være noe begrenset i dag. Som vi har sett, så legger teorien til grunn et mer omfattende databegrep enn det som er lagt til grunn i

⁴² Stein Schølberg i artikkelen ”Data kriminalitet og Internett” 1995 s 4

⁴³ Kontinuerlig strøm av data som vises mens nedlastningen pågår.

dekoderdommene. Som DVD-dommen viser, så ønsker heller ikke domstolene å kommentere dekoderdommenes tolkning av databegrepet.

Det er også vært å merke seg den sterke dissensen som man hadde i dekoderdommen I. I dag har man også en egen straffebestemmelse i straffelovens § 262 som omfatter slag og markedsføring av piratsmarkert. Hadde en slik sak kommet opp i dag, så ville man ikke ha prøvet den mot § 145 annet ledd, men gått direkte til § 262.

Som nevnt i innledningen så er en revisjon av § 145 annet ledd er på vei. De eventuelle endringene her, vil kunne medføre at dekoderdommene mister sin relevans.

Etter min mening, så er dekoderdommenes tolkning av "data" uheldig, og mye taler for at man bør ilegge en så innskrenkende som det lar seg gjøre. Et eksempel på en situasjon som kan oppstå i dag, som en følge av disse dommene vil være at man kan se et fjernsynsprogram på en datamaskin med fjernsynsmottaker, og se det samme programmet fra internett på den samme datamaskinen samtidig. Overføringene vil i begge tilfeller kunne være over den samme kabelen, men kun et av dem vil falle inn under databegrepet i § 145 annet ledd.

På den annen side, så kommer man ikke bort fra at vi har to rettskraftige Høyesterettsdommer, som sier at kringkasting av fjernsynssendinger ikke er "data", og det er rettstilstanden i dag.

3 Uberettiget adgang.

For at en handling skal være omfattet av straffeloven § 145 annet ledd, så må man ikke bare ha brutt en beskyttelse, adgangen må også være "uberettiget".

Skyldkravet er forstøtt jfr. straffelovens § 40. Man kan således ikke uaktsomt skaffe seg en uberettiget adgang, til data, og bli omfattet av § 145 annet ledd.

3.1 ”Uberettiget”

Det må presiseres hva som må være uberettiget, for at § 145 skal komme til anvendelse. Når det her er snakk om uberettiget adgang, så er det ikke adgangen i seg selv som skal være uberettiget. Det er det å gjøre seg kjent med dataene som skal være uberettiget, og ikke måten adgangen ble oppnådd på. I forarbeidene⁴⁴ eksemplifiseres dette ved å uttale; ”Uttrykket «uberettiget» knytter seg til de enkelte opplysninger og ikke til dataanlegget som sådant.”. Uberettighetskravet blir således heller ikke avhengig av om selve adgangen er ulovlig eller ikke. Man må ikke ha brutt seg inn i en datamaskin, for at adgangen skal bli uberettiget. I DVD-dommens tilfellet er det altså være adgangen til filmen, som må være uberettiget.

Selve utnyttelsen av dataene er heller ikke en del av vilkåret om ”uberettiget” i § 145. Det sentrale er det at man her tilgang til dataene. I forarbeidene⁴⁵ tar man frem et eksempel om at en ansatt som har rettmessig tilgang til fortrolig informasjon, som han så selger. Dette tilfellet vil ikke bli omfattet av § 145. Dette fordi, selv om utnyttelsen av informasjonen er uberettiget, så var den ansatte berettiget til å ha kjennskap til informasjonen.

Som nevnt over, viser også NDD-dommen⁴⁶ at det ikke er et krav om at man skal ha gjort seg kjent med innholdet, for at man skal være ansett for å ha skaffet seg uberettiget adgang. Det vil for eksempel være tilstrekkelig å bryte seg inn i en database. Man må ikke gjøre seg kjent med innholdet i databasen for at § 145 skal komme til anvendelse.

Loven er jo for eksempel ikke ment å ramme personer som bryter seg inn til steder man har rett til å være. Et eksempel på et grensetilfellet vil kunne være at min advokat mottar et brev, som er adressert til ham. Jeg vet at jeg skal bli gjort kjent med innholdet, så jeg åpner brevet. Det kunne her stilles spørsmål ved om jeg i dette tilfellet ville være berettiget til å skaffe meg adgang til innholdet?

⁴⁴ NOU 1985:31 side 15 punkt 5.2.4.

⁴⁵ NOU 1985:31 side 15 punkt 5.2.4

⁴⁶ LB-1997-1527

3.2 *Hva forstår man med uberettiget?*

Etter en normal språkforståelse, så vil ”uberettiget” bety at en har fått tilgang til data, som en ikke har rett til å gjøre seg kjent med. Med andre ord, så må tilgangen være forbudt. Det kan spørres om dette er sammenfallende med en normal rettsstridsreservasjon. Dette synet får støtte i forarbeidene til lovendringen av straffelovens § 145 i 1987, hvor det uttales:

”Generelt må kravet om at innsynet skal være uberettiget forstås som en vanlig rettsstridsreservasjon, som henviser først og fremst til normer utenfor strafferetten.”⁴⁷

Flere steder i straffeloven vil man finne bestemmelser som inneholder rettsstridsreservasjoner. Typiske formuleringer brukt av lovgiver vil kunne være ord som, ”ulovlig”, ”uberettiget” eller ”rettsstridig”. Valg av ord å bruke her, kan nok i enkelte tilfeller bli litt tilfeldig, men innholdet av rettsstridsreservasjonen er nok den samme. Et eksempel på dette vil kunne være straffelovens § 90 første ledd og § 91 første ledd. I det første tilfellet blir uttrykket ”rettsstridig” brukt. Lovgiver har så i § 91 annet ledd valgt å bruke ”uberettiget”. I Rt. 1979-1492 kommenterer høyesterett akkurat disse paragrafene, og utaler på side 1499; ”Slik jeg ser det, ligger det imidlertid ingen realitetsforskjell i dette ordvalget.” Det strafferettsbestemmelsen her gjør er å vise til andre regler eller normer, og lar de få mulighet til å gi strafferettslige sanksjoner.

Forarbeidene viser dermed for det første at det ikke er nødvendig at en strafferettslig regel skal være brutt, for at innsynet skal være å anse som uberettiget. Man vil da kunne gå til andre rettsområder, eller til avtaler som ligger til grunn, i fastsettelsen av om en adgang var uberettiget eller ikke. I forarbeidene til straffeloven blir

⁴⁷ Ot.prp.nr.35 1986-1987 s.21

rettsstridsreservasjoner sett på som en henvisning til regler i annen lovgivning utenfor strafferetten, jfr. SKM 1896 s 98. Dette er dog fra de eldste forarbeidene til straffeloven, og det har naturlig nok vært forandringer i strafferetten siden disse forarbeidene. Man har gjennom rettspraksis i dag fått en videre forståelse av rettsstridsbegrepet.⁴⁸

For det andre så blir det et spørsmål om man kan tolke forarbeidene til at også brudd på ikke-rettslige normer som begrenser adgangen til data, vil kunne medføre at adgangen kan bli uberettiget. Det vil da for eksempel være adgang i strid med interne regler i en bedrift eller organisasjon, som setter begrensninger for hva ansatte skal ha adgang til av data. Hvis man så skaffer seg tilgang til informasjon som det ikke er ment at man skal ha tilgang til, etter interne regler, så vil denne adgangen kunne bli å kategorisere som uberettiget. En slik tolkning får støtte i Ot.prp.nr.35 1986-1987 s.21 femte avsnitt, hvor det blant annet blir uttalt at tolkningen av ”uberettiget”, må ta utgangspunkt i rettslige regler og normer som måtte gjelde. Som eksempler nevnes også ”(...) arbeidsrettslige regler, tariffavtale, arbeidsavtale og stillingsinstruks (...)”⁴⁹ Dette er ikke en uttømmende liste.

Et praktisk eksempel vil kunne være at man åpner et brev, som er adressert til en annen person. Det å åpne brevet vil være uberettiget, med mindre man har holdepunkter for noe annet. En sekretær vil for eksempel normalt ha stillingsfullmakt til å åpne innkommende brev. Selv om de ikke er adressert til sekretæren selv.

Et annet spørsmål er om uskrevne normer også vil kunne bli tatt i betraktning. Et eksempel på at dette kan vi finne i den såkalte Norman Data Defence dommen (NDD-dommen). Saken var her det at i forbindelse med et innslag i Dagsrevyen om datasikkerhet, tok en ansatt ved Norman og testet sikkerheten til Universitetet i Oslo. Dette var for øvrig ikke avtalt med Universitetet. Dette ble oppdaget av Universitetet, og sett på som et forsøk på innbrudd. Sakkyndige uttalte i herredsretten at det finnes normer for hva som er uhøflig å gjøre ovenfor andre på nettet. Dette viser at uskrevne normer kan være med på å klargjøre om en handling er uberettiget. Nå bør det nevnes at

⁴⁸ Se Slettan / Øie – Forbrytelse og straff s 76-77.

⁴⁹ Ot.prp.nr.35 1986-1987 s.21 femte avsnitt.

de tiltalte i NDD-dommen, ble frifunnet for overtredelse av straffelovens § 145 i senere instanser. Bakgrunnen for frifinnelsen var at programmene som ble kjørt, ble ansett for ikke å kunne gi adgang til ”data”. Dette med unntak av den tiltaltes forsøk på oppkobling ved bruk av brukernavnet ”guest”. Dette ville dog også falle utenfor § 145. Dette fordi hvis det hadde gitt tilgang, så hadde det vært fordi Universitetet hadde åpnet for bruk av en slik gjestekonto, og det ville således heller ikke være snakk om et innbrudd.⁵⁰ Det bør dog nevnes at NDD-dommen har blitt kritisert i den juridiske litteraturen for å gått litt langt i å tillate føling etter svakheter i et datasystem.

Forarbeidene sier at fortolkningen av ”uberettiget” må ”(...) ses i sammenheng med kravet om at gjerningsmannen må ha overskredet en eller annen form for beskyttelse eller hindring.”⁵¹ Det kommer da i tillegg til kravet om at man skal ha omgått en form for beskyttelse, som er en forutsetning for at annet ledd i § 145 skal kunne komme til anvendelse. Her ser vi nå at denne omgåelsen også blir en tolkningsfaktor i om adgangen var uberettiget. En følge av dette vil da kunne bli at, jo bedre beskyttelsen har vært, og jo mer arbeid som ligger i å bryte den, jo mer sannsynlig er det at man anser adgangen til å være uberettiget.

3.3 Hva en er en beskyttelse.

For at § 145 annet ledd skal kunne komme til anvendelse, så må gjerningsmannen ha brutt en eller annen form for beskyttelse når han skaffet seg tilgang til data. Alternativt til å bryte en beskyttelse, vil den som på en ”lignende måte”, uberettiget skaffer seg adgang til data, også bli rammet.

Her ser vi at det må ligge foreligge en form får beskyttelse rundt dataene. Har det ikke blitt gjort noen forsøk på å hindre at andre får tilgang til dataen, vil straffeloven § 145 vanskelig kunne komme til anvendelse. I forarbeidene til endringen i 1985 uttales det;

⁵⁰ Jfr. LB-1997-1527.

⁵¹ Ot.prp.nr.35 1986-1987 s.21 femte avsnitt.

”Forutsetningen for det strafferettslige vern etter § 145 er at den berettigede selv har gjort noe for å beskytte seg mot inngrep fra uvedkommende”.⁵²

Videre sies det,

”Først når det er tatt rimelige foranstaltninger i så måte, kan han kreve hjelp fra strafferettsapparatet.”⁵³

3.3.1 Hvilke krav stilles en beskyttelse

Man må nok her også kunne sette krav til eventuelle passord, får at det skal kunne oppfylle vilkårene til å gi beskyttelse. Passord i seg selv er ikke en beskyttelse, men en måte å få tilgang på, gjennom beskyttelsen. Hvis man for eksempel har data på firmaets nettverk som man ikke ønsker at alle ansatte skal ha tilgang til, så må heller ikke alle kunne få adgang ved å bruke sitt standard passord. Bare det at det er et passord, er selvsagt ikke nok til å gjøre adgangen uberettiget. Det kan nok også stilles spørsmål om kvaliteten på passordet, kan ha betydning. Hvis man for eksempel kan få tilgang til dataen ved bruk av brukernavn og passord som ”Anonymous” eller ”Guest”, så vil nok dette neppe gi beskyttelse. Slike passord brukes typisk ved tilgang til FTP-Tjenere⁵⁴. Dette ble jo også tilfellet NDD dommen, som jeg nevnte over. Her ble et forsøk på å få tilgang til en server med bruk av gjestepassord ikke ansett for å kunne gi uberettiget adgang til data. Her er det da meningen av systemet skal være åpent. De fleste servere tillater dog ofte ikke at man ikke har noe passord. Derfor har man ofte slike standardpassord på de områdene som man ønsker at skal være tilgjengelig for allmennheten.. Hvis det skal trekkes en grense, så vil nok den gå der hvor man ikke lett kan gjette seg til hva passordet er. Et eksempel kan være at man blir bedt om å skrive inn passord, men at det holder med å trykke ok. Man kan også tenke seg administratoren

⁵² NOU 1985:31 – Datakriminalitet side 31, venstre spalte, tredje avsnitt.

⁵³ NOU 1985:31 – Datakriminalitet side 31, høyre spalte, andre avsnitt.

⁵⁴ File Transfer Protocol – En filoverførings protokoll som er mest brukt på internett, når man skal overføre data, i form av filer.

har fått et lite ønske om å være humoristisk, og har valgt passordet "Passord" eller "Password". Når brukeren så skal logge seg på, så blir man møtt med spørsmålet "Vennligst skriv passord:". Hvis man så skriver "Passord", så får man tilgang. Et annet eksempel vil være administratoren har brukt det klassiske passordet/brukernavnet "Gud". Det kan spørres om disse eksemplene er for enkle til å kunne fremstå som en beskyttelse.

Det kan spørres om det er oppstilt et minstekrav til kvaliteten eller effektiviteten av beskyttelsen. I forslag til ny åndsverkslov⁵⁵, så har man innført et begrep om omgåelse av "(...) effektive tekniske beskyttelsessystemer (...)". Her sier man at innenfor en viss rimelighet, så må beskyttelsen faktisk kunne stoppe noen fra å få adgang, for å kunne anses som effektiv. Et minimum må under enhver omstendighet være at gjerningsmannen må gjøre noe aktivt for å få adgang. Eksempelt med at man blir fortalt at adgangen til informasjonen er begrenset, vil da være en effektiv teknisk beskyttelse. I dekodeorddommen I⁵⁶, så var det som skulle hindre uvedkommende adgang, støy på sendingen. Man sendte ut fjernsynssignalene på vanlig måte, men man la til støy på sendingen. Kunder av fjernsynsselskapet fikk så en dekode som kunne fjerne denne støyen fra sendingen igjen. Dette kan ikke sies å være en spesielt avansert form for hinder, som viste seg å være relativt enkelt å omgå. Likevel, valgte Høyesterett å godta dette som en tilstrekkelig sikring.

Man må kunne anta at et brudd på en sterk beskyttelse lettere vil bli å anse som uberettiget adgang enn hvis man omgår en enkel beskyttelse. Hvis det ligger informasjon på datanettverket som det ikke er mening at man skal ha tilgang til, men man allikevel kommer inn med sitt normale passord, så kommuniserer dette veldig dårlig til brukeren at han ikke er berettiget til informasjonen. I DVD-dommen kommenterer lagmannsretten også at sikkerheten i CSS er svak.⁵⁷ Dette eksemplifiseres ved at et vitne, Stevenson, foretok en kryptoanalyse av CSS. Der konkluderte han at, selv om krypteringen er på 40 bit, så er den så svak at den i realiteten ikke gir bedre beskyttelse

⁵⁵ Ot.prp.nr.46 2004-2005 s166 "Nytt kapittel 6a"

⁵⁶ RT-1194-1610

⁵⁷ DVD-dommen - avsnitt 6 i vedlagt kopi.

enn en 16 bits nøkkel. Han laget så et program som kunne knekke en slik vilkårlig nøkkel på under et sekund.

Jeg kan ikke helt se at dette skal være av noen stor betydning i forhold til straffeloven § 145, 2.ledd. For det første, må man kunne si at CSS uansett er en sterkere beskyttelse en for eksempel kodingen av fjernsynssendinger ved å tillegge støy, noe som har blitt godtatt av Høyesterett som tilstrekkelig i dekommerdommene. For det andre kan vi, hvis vi sammenligner med første ledd, se at der er det tilstrekkelig at et brev blir brutt opp, det kreves mye mer kunnskap og arbeid for å knekke en kode som CSS. Det ville være litt som å møte en anklage om innbrudd, ved å si at låsen på døra var svært dårlig og lot seg lett bryte opp, og at det dermed ikke er å anse som et innbrudd. Det sentrale bør således kunne sies å være at man må foreta seg noe aktivt for å kunne sies å ha brutt seg inn. Man kan ikke unngå å legge merke til sikkerhetstiltakene rundt DVD-filmen. Man kan ikke bryte den uten å vite at man faktisk prøver å omgå den, og det bør være nok til å vekke spørsmål om man faktisk skal ha adgang til dataen bak beskyttelsen.

Det synes etter dette, ganske klart at det ikke stilles veldig strenge krav for at man skal kunne godta en beskyttelse som god nok. Man må nok også kunne se at CSS er en god nok beskyttelse i så måte, selv om det har vist seg at den er forholdsvis lett å bryte.

3.3.2 På lignende måte.

I NOU 1985:31 la man til et annet ledd i § 145, men kun med vilkåret ”(...)å bryte en beskyttelse(...)”. I Ot.prp.nr35 (1986-1987) var man ikke helt fornøyd med denne ordlyden, da man mente at den kunne komme til å ramme for snevert. Man la dermed til ”(...) eller på liknende måte(...)”. Videre sies det;

”Ved tolkingen av « på liknende måte » må man se hen til hva som ligger i kravet om å bryte en beskyttelse. Som « beskyttelse » må reknes både vanlige avstengningsmekanismer som f eks maskinlåser, og dessuten koder og passord

som er lagt inn med samme formål. Kravet om at beskyttelsen skal « brytes » innebærer at beskyttelsen må omgås eller settes ut av funksjon på irregulær måte.”⁵⁸

Som nevnt over, så må det også være satt opp en eller annen form for beskyttelse ”rundt” dataen, som gjerningsmannen skal ha brutt for å få adgang til dataen. Ved at man la til ”på liknende måte” i § 145, så har man laget et alternativ til å *bryte* en beskyttelse. Det må således fortsatt foreligge en beskyttelse. Man sier videre i forarbeidene at ”(...) § 145 bare skal ramme tilfelle hvor det å skaffe seg adgang til data må karakteriseres som kvalifisert uberettiget.”.⁵⁹ Dette tyder på at adgangen må være åpenbart uberettiget, for at straffelovens § 145 annet ledd skal komme til anvendelse når man bruker alternativet ”på lignende måte”. Et eksempel her vil være at man har tilegnet seg en falsk identitet, og på bakgrunn av denne får tildelt brukernavn og passord. Når man så skaffer seg tilgang til data, så har man ikke brutt beskyttelsen, men åpnet den på regulært vis. Lovgiver ønsket at en slik adgang også skulle være omfattet av § 145 annet ledd, og la dermed til ”på lignende måte”, som ville ramme et slikt tilfelle som nevnt over.

I A-Tekst-dommen⁶⁰ finner retten at den tiltalte ”på lignende måte” har skaffet seg adgang til ”data”. Kort fortalt så var faktum her Aftenpostens nettavis hadde en betalingstjeneste som tillot søk i tidligere utgitte artikler. Den tiltalte hadde ikke tilgang til å bruke tilbudte søkemotoren, men han observerte at ved å gjøre forandringer i IP-adressen, så kunne han få direkte tilgang til artikler, dog uten den sortering som bruk av søkemotoren ville ha gitt. Retten finner at dette faller inn under ”på lignende måte”. Jeg tror denne dommen går litt langt. Det kan blant annet stilles spørsmål ved om det finnes en tilstrekkelig beskyttelse, når man kun blir hindret adgang til dataene ved uberettiget bruk av søkemotoren. Som nevnt over så er det et krav om at man har ”(...) selv har gjort noe for å beskytte seg mot inngrep fra uvedkommende”.⁶¹ Og at, ”Først når det er

⁵⁸ Ot.prp.nr35 (1986-1987) s 20 siste avsnitt,

⁵⁹ Ot.prp. nr. 35 1986-1987 s.20 siste avsnitt

⁶⁰ TPBYR-1997-01449 - Skien og Porsgrunn byrett.

⁶¹ NOU 1985:31 – Datakriminalitet side 31, venstre spalte, tredje avsnitt.

tatt rimelige foranstaltninger i så måte, kan han kreve hjelp fra strafferettsapparatet.”⁶²

Hvis man kan skaffe seg adgang kun ved å forandre IP-adressen, så er vel dette neppe å anse som en beskyttelse. Spesielt med tanke på at man ved uaktsomhet kan komme til å få adgang til dataene. Det er for eksempel ikke uvanlig at hvis man er inne på en internettside, som oppdateres daglig, at man vil se adresselinjen inneholder en dato. Hvis man så ønsker å se gårsdagens utgave av siden, kan man bytte ut et tall, i det som representerer datoen. Hvis man på en så enkel måte kan få tilgang, så taler ikke det for at man har implementert en beskyttelse.

Som nevnt over så er det et krav om forsett for anvendelsen av § 145. Under en hver omstendighet så vil ikke beskyttelsen kunne anses for å være tilfredsstillende, hvis man kan omgå den med en tilfelijkheid, som å taste inn en IP-adresse.

3.4 Vil bruk av DeCSS kunne være berettiget?

I DVD-dommen ble det et spørsmål om adgangen til filmen, som programmet DeCSS ga brukeren, var å anse som ”uberrettiget”. Filmen som den tiltalte hadde brukt DeCSS på var en film som han hadde kjøpt på lovlig vis. Han var således i sin fulle rett når han ønsket å se filmen. Selv om den tiltalte bryter beskyttelsen, så vil han fortsatt være berettiget til å se filmen, og § 145 annet ledd vil så ikke kunne komme til anvendelse.

For det første så vil en bruk av DeCSS medføre at det blir fremstilt et ukryptert eksemplar av filmen på datamaskinens harddisk. Der med oppstår det et spørsmål om en slik eksemplarfremstilling er tillatt.

Det blir så et spørsmålet om det at den tiltalte bruker et uautorisert avspillingsutstyr gjør at adgangen til dataen blir å anse som ”uberrettiget”. Dette blir også nevnt av

⁶² NOU 1985:31 – Datakriminalitet side 31, høyre spalte, andre avsnitt.

lagmannsretten⁶³. Spørsmålet reiser i sammenheng med en lovlig bruk av DeCSS to problemer. For det første, om den tiltalte kan bli kontraktsmessig bundet til å kun se filmen på autorisert avspillingsutstyr. Da spesielt gjennom kontraktskonstellasjon som etikettering. Herunder om ett brud på en slik kontrakt vil gjøre adgangen uberettiget.

3.4.1 Tillater åndsverksloven bruk av DeCSS?

I det følgende vil jeg da legge til grunn at det ikke vil være noe kontraktsmessig hinder for å bruke uautoriserte avspillingsutstyr. Det blir da et spørsmål om hvorvidt DeCSS har egenskaper som skulle gjøre enhver bruk av programmet uberettiget.

Som nevnt over vil enhver bruk av DeCSS lage en kopi av filmen på datamaskinens harddisk. Det klare utgangspunkt er at eksemplarframstilling er en enerett som tilfaller opphavsmannen eksklusivt, jfr. Åndsverksloven § 2. Man kan få rett til eksemplarframstilling gjennom avtaler med rettighetshaver eller ved eventuelle unntak gitt ved lov. Et unntak fra denne hovedregelen finnes i åndsverksloven § 12. Her åpnes det for at man kan fremstilles eksemplar av enkelte åndsverk, selv når man ikke har noen avtale med rettighetshaver om en slik bruk, når dette skjer til privat bruk, og ikke i ervervsøyemed. Det å fremstille et eksemplar av en film til privat bruk, faller innenfor rekkevidden av § 12. Film er heller ikke omfattet av unntakene fra § 12 i annet ledd.

Lagmannsretten legger til grunn at formålet med datamaskinprogrammet var å skaffe en avspillingsmulighet av dvd-filmer, og ikke spredning av dem. Således var den tiltalte berettiget til å fremstille ett eksemplar av filmen etter strl. § 145. Det kan dog oppstå andre begrensninger av retten til eksemplarframstilling. Det kan dog nevnes at det i praksis er mulig å implementere DeCSS i en avspiller, så DeCSS kunne dekryptere filmen mens den ble spilt av. Man ville i så fall kunne slippe å lage et eksemplar av filmen, og således under en hver omstendighet ikke bli omfattet av § 12, da avspilling innen det private området faller utenfor opphavsmannens enerett etter åndsverksloven

⁶³ DVD-dommen - avsnitt 19 flg. i vedlagt kopi.

§ 2. En slik implementering av DeCSS forelå dog ikke ved tidspunktet for saksanleggelsen.

3.4.1.1 Hvor mye av verket kan kopieres?

Lagmannsretten tar opp spørsmålet om privatbruksregelen i åndsverksloven § 12 tillater en slik bruk som en bruk av DeCSS vil innebære⁶⁴. Åndsverksloven § 12 gjør et unntak fra § 2, og hjemler en rett til privat eksemplarframstilling av åndsverk. Det blir av lagmannsretten reist spørsmål ved om privatbruksretten i åndsverksloven § 12 gir rett til å kopiere et åndsverk i sin helhet. Hvis det viser seg at man ikke kan lage en komplett kopi av hele verket, så vil dette kunne resultere i at en bruk av programmet ikke kunne brukes uten å stride mot strl. § 145 annet ledd, ved at adgangen ville bli ”uberettiget”.

Det blir så et spørsmål om regelen om rett til kopiering til privat bruk i åndsverksloven § 12, har begrensninger i hvor stor del av verket man har rett til å kopiere. Gjelder den for hele verk eller kun begrensede deler av det? Lovtekstens ordlyd, taler ikke ikke for at det skal være noen begrensning i hvor mye av et verk man kan kopiere. Loven tillater at ”(...) enkelte eksemplar av et offentliggjort verk fremstilles til privat bruk.”⁶⁵ Det nevnes her at man kan lage et eksemplar av et verk. Ettersom man ikke gir mer uttrykk for noen begrensninger, taler det for at man kan ha en rett til å kopiere hele verket. Videre er det heller ikke alle verk som lar seg bruke, hvis man prøver å dele det opp. Et eksempel på dette vil kunne være hvis man tar et bilde eller avstøpning av et kunstverk, så vil man kunne ta bilde av hele verket, ikke bare deler av det. Dette da under forutsetning av at det ikke ville stride om § 12 annet ledd bokstav d.

I forarbeidene til åndsverksloven § 12 er det dog tatt til ordet for at det kan finnes en begrensning i hvor mye av et verk man kan fremstille et eksemplar av.⁶⁶ Det nevnes for

⁶⁴ DVD-Dommen - avsnitt 22 i vedlagt kopi.

⁶⁵ Åndsverkslovens av 2000 nr. 52. § 12 første ledd.

⁶⁶ Ot.prp.nr.15 (1994-1995) side 38, siste avsnitt.

eksempel at, ”Hvor stor del av et verk og antall eksemplar som kan fremstilles, vil bero på omstendighetene i det konkrete tilfelle”. Videre blir det sagt;

”For eksempel vil det normalt ikke være adgang til for personlig bruk å fremstille selv en enkelt kopi av en hel bok, eller et helt tidsskrift som er å få i handelen.”

Som en følge av presumsjonsprinsippet vil Bernkonvensjonens art. 9 kunne være et viktig tolkningsmoment for rekkevidden av § 12. Presumsjonsprinsippet er et prinsipp som bygger på at man antar at norsk internrett til enhver tid stemmer overens med våre internasjonale forpliktelser. Man vil da tolke norsk internrett i lys av de internasjonale avtaler vi har inngått på området. Man vil da oppnå en større harmoni mellom reglene. Første ledd i Art. 9 kommer til uttrykk gjennom åndsverkslovens § 2. Artikkel 9s andre ledd tillater dog unionslandene å ha særregler som kan bryte fra første ledd, i enkelte situasjoner.

Det er allikevel satt grenser for hvor langt medlemslandene kan gå i å gi unntak fra art. 9. første ledd, i den interne lovgivningen. Lover basert på unntakene i art. 9 annet ledd, må oppfylle den såkalte ”tretrinns testen”, for å ikke bli konvensjonsstridig. For det første må det være snakk om en regel som kun omfatte spesielle tilfeller, ”special cases”. Videre må en eventuell eksemplarframstilling ikke skade den normale utnyttelsen av verket, jfr. ” (...) provided that such reproduction does not conflict with a normal exploitation of the work (...)”. For det tredje må ikke eksemplarframstillingen tilsidesette opphavsmannens legitime interesser, jfr. ”(...) not unreasonably prejudice the legitimate interests of the author.”

Kravet om ”spesielle tilfeller”, viser til at regelen skal være begrenset til å kun å omfatte spesielle tilfeller, ”special cases”. Man har her ikke ment å gjøre unntak for enkelttilfeller, men for enkelte situasjoner. Det er også meningen her å sette en stopper for for vide og omfattende unntak. Eksempler på unntak som man implementert i norsk

rett på dette grunnlag vil kunne være reglene for bibliotek, privat eksemplarframstilling, eksemplarframstilling i undervisning med mer⁶⁷.

Videre må ikke unntaket gå ut over opphavsmannens normale utnyttelse av verket. Kanskje det viktigste for rettighetshaver, vil være å få vederlag for utnyttelse av verket. Unntakene som blir gitt bør således ikke føre til at opphavsmannens potensielle salg svikter. Unntak for bibliotek og privat eksemplarframstilling vil kunne gi et teoretisk tap for opphavsmannen. Man har derfor i noen tilfeller opprettet egne avgifter eller overføringer fra staten, i form av avtalelisensordninger, som en form for kompensasjon.

Til sist må regelen heller ikke på en urimelig måte tilsidesette opphavsmannens legitime interesser. Her har man tatt sikte på å beskytte opphavsmannens ideelle rettigheter. Den mest grunnleggende rett vil være for opphavsmannen å få sitt navn på verket, om han så ønsker. Dette er nok ikke den retten som er mest utsatt av opphavsmannens rettigheter.

Dette medfører at man kan ha en internrettslig regel om privat eksemplarframstilling, så lenge den ikke strider mot art. 9, noe den i mitt syn ikke kan sies å gjøre. Det at noen tar en sikkerhetskopi av en film de selv har ervervet, vil ikke skade opphavsmannen interesser i nevneverdig grad. Hvis jeg kopierte en bok til privat bruk, så vil dette kunne gå ut over opphavsmannen. Opphavsmannen kan da ha lidt et potensielt tap ved at jeg ikke kjøpte boken. Lovgiver har i dette tilfellet valgt å la privatpersonens interesser veie tyngre.

Etter min vurdering burde man kunne ha en lignende anvendelse av regelen på en film, som en bok. Det å lage en kopi av en film til privat bruk, vil ikke ramme rettighetshaveren i nevneverdig grad. Det burde dermed heller ikke være nødvendig å gjøre som lagmannsretten gjør, å skille mellom en bok og en film, ut i fra mediet åndsverket er lagret/nedskrevet på.

⁶⁷ Se åndsverkslovens annet kapittel.

Lagmannsretten tar til ordet for at det tillatt å lage et eksemplar av hele filmen etter § 12. Dette blir blant annet begrunnet med at det er en vesentlighets forskjell mellom en film og en bok. Retten trekker også fram at det er en del egenskaper ved mediet filmen er lagret på, som gjør den særlig utsatt for skader.⁶⁸ Retten sier videre "Lagmannsretten legger til grunn at en DVD-plate er så utsatt for å få skader at kjøperen må være berettiget til å ta en kopi,". Lagmannsretten argumenterer her for en slags sikkerhetskopifunksjon som man har for datamaskinprogrammer i åndsverksloven § 39h annet ledd.

Det kan stilles spørsmål ved om DVD mediet virkelig er så utsatt for skader som retten skal ha det til. Hvor lang levetid har man egentlig krav på at en DVD-plate skal ha? Kan ikke det samme sies om en bok. Sider kan falle ut, eller et ikke ukjent fenomen at man mister den i badekaret. Det skal sies at små skader på et digitalt medium kan føre til at hele mediet blir uleselig, og sånn sett vil fort konsekvensene av en liten skade bli store.

Et annet spørsmål blir da om § 12 kan anvendes hvis man ønsker å ta en kopi av en film fra en VHS kassett. Ville dette skifte av medium forandre lagmannsrettens syn på saken? Dette da under den forutsetning av at man kan si at en VHS kassett er mer slitesterk enn en DVD-plate.

Etter min vurdering foreligger det ikke en begrensning i hvor mye av et verk man kan kopiere med utgangspunkt i åndsverksloven § 12.

3.5 Salg med forbud mot kopiering.

Problemstillingen her er om det gyldig kan avtales innskrenkninger i retten til privateksemplarframstilling. Som jeg var inne på over, under 3.1.2 så vil avtaler kunne

⁶⁸ Se DVD-dommen vedlagt kopi avsnitt 31.

være med på å finne definere en rettsstridsreservasjon. Et brudd på en eventuell på en slik avtale vil så kunne medføre at bruken av DeCSS vil være uberettiget.

Det reises her i utgangspunktet to spørsmål. For det første om man vil kunne godta slike kontraktsvilkår i kontraktsretten. Her under kan det spørres om man skal godta en slik ”privat lovgivning”, som begrenser de rettigheter lovgiver har gitt forbrukeren i loven. For det andre er det et spørsmål om man kan bli kontraktmessig bundet av en slik klausul når denne kommer som en følge av etikettering. Det kan også være at situasjonen arter seg forskjellig for kjøp over internett enn ved en mer ordinær kontraktsslutning.

Utgangspunktet er at etter norsk rett, så har man en full avtalefrihet på formuesrettens område, jfr. NL 5-1-2. Dette taler for at man kan avtale seg bort fra muligheten til privat eksemplarframstilling etter åndsverksloven § 12. For øvrig er også åndsverkslovens § 12 deklarasjonsmessig, den kan således fravikes ved avtale, etter partenes ønsker.

Det som dog kan skape problemer, er når en part ensidig nedsetter generelle forbehold i avtalen. Da gjerne uten noen form for kompensasjon for den annen part. For det første så kan dette lede til at deler av avtalen blir tilsidesatt av retten med hjemmel i avtaleloven § 36. Dette er noe jeg vil ta for meg nedenfor. For det annet har man i forarbeidene til åndsverksloven tatt til motmæle mot dette. Dette synet sier man er støttet i reelle hensyn. I NOU 1983:35 side 62-63 uttales det;

”Utvalget mener at det som gjeldende rett må leddes til grunn at ensidig forbehold mot bruk som er tillatt etter åndsverksloven, i alminnelighet ikke kan anses gyldig.”

Man understøtter sitt syn videre med å påpeke at et dette kan sammenlignes med en privat lovgivningsvirksomhet. Ved å godta det vil man kunne fjerne mye av den interesseavveining som er lagt til grunn i loven. Dette punktet tas også opp i DVD-

dommen⁶⁹. Disse argumentene ble også fremhevet i forarbeidene til endringene i åndsverksloven i 1990, jfr. Ot.prp.nr.33 (1989-1990) side 20 siste avsnitt.

Videre støtte for dette kan man finne i Ot.prp.nr.34 1987-1988 s 21, hvor det uttales;

”Utvalget antar videre at rettighetshaverne etter gjeldende rett i alminnelighet *ikke* kan ta *ensidige forbehold* mot bruk som er tillatt etter åndsverkloven, jf innstillingen kap V.4.3.2. f s 62-63. Klausuler mot viderespredning på de enkelte eksemplar av masseproduserte videogram vil derfor i alminnelighet være uten betydning, i og med at de vanligvis ikke kan anses for kontraktsmessig vedtatt.”

og...

”*Justisdepartementet* slutter seg til utvalgets argumentasjon og syn på at ensidige forbehold på de enkelte eksemplar av verket overfor bruk som er tillatt etter åndsverkloven, i alminnelighet ikke kan anses gyldige.”

Lovgiver skepsis til å tillate forbehold mot reglene i åndsverksloven kommer her tydelig frem. Men det er dog verdt å merke seg at man i disse uttalelsene har snakket om ”ensidige forbehold”. Det vil da kun være forbrukeren som oppgir rettigheter han har, uten å få noen form for kompensasjon for det. Dette vil typisk være tilfeller hvor man står ovenfor etikettering eller standardavtaler. Rettstilstanden ser ut til å være at man er tilbakeholden med å godta slike vilkår, men at det vil være mulig, hvis det ikke fremstår som urimelig.

3.5.1 Etikettering.

Det er spesielt to momenter som ved ”shrink-wrap” klausuler som kan få betydning hvis en domstol skal vurdere gyldigheten av avtalen. For det første så er etikettering er en

⁶⁹ DVD-dommen – avsnitt 27 i vedlagt kopi.

form for standardavtale⁷⁰, med de tolkningsmomenter som det kan medføre, noe som jeg ikke vil gå inn på i denne oppgaven. For det annet så vil det bli spørsmål om når og om vedtagelsen av avtalen har funnet sted.

Med etikettering så tenker man på de tilfeller hvor kjøper blir presentert med nye kontraktsvilkår ved levering. Disse er da gjerne trykt på produktet eller lagt ved inne i forpakningen til produktet som kjøpes. Et annet mye brukt uttrykk for den samme kontraktskonstruksjonen, er shrink-wrap avtaler. Shrink-wrap navnet ble originalt brukt om avtaler som medfølgte masseproduserte datamaskinprogramvare. Kjøper blir her ikke kjent med kontraktsvilkårene før etter man har brutt innpakningen. Kjøper vil dermed i mange tilfeller heller ikke være klar over at nye kontraktsvilkår vil bli presentert etter avtaleslutningen. Navnet kommer av måten produktet er pakket på. Innpakningen er typisk en pappeske som igjen er omgitt av plast. Plasten krympes rundt esken ved at den utsettes for varme, derav "shrink-wrap". Tanken er da at kjøper aksepterer de vedlagte klausulene ved å bryte innpakningen, eller åpne konvolutten hvor program-CDen ligger.

Det er nok flere grunner til at man fremmer kontraktvilkår på denne måten. For det første, så kan det være et forsøk på få kjøperen til å faktisk lese og gjøre seg kjent med vilkårene. De fleste forbrukere har ikke en inngående kjennskap til bakgrunnsretten, så en innføring av rettigheter og plikter kan være ønskelig. Dette vil kunne være tilfellet når vilkårene er sammenfallende med bakgrunnsretten. For det andre så kan det også være et forsøk fra selgers side til å skaffe litt bedre vilkår enn det som finnes i lovgivningen. Man hører for eksempel ofte om leverandører som når de blir stilt ovenfor et spørsmål om reklamasjon, viser til standardavtalen hvor man kun har ett års garanti. Dette da i håp om at forbrukeren ikke skal se forskjellen på en garanti- og en reklamasjonssak.

Noen ganger gir de også kjøperen en videre rett, enn det han i utgangspunktet har krav på etter den nasjonale lovgivningen. Det kan spørres hvorfor dette blir gjort. Det å ha gode

⁷⁰ Se Hov, Jo – avtaleslutning og ugyldighet kap. 6 - VI

vilkår i en "shrink-wrap" avtale er ikke en spesielt gunstig måte å reklamere for seg selv på. Eventuelle kjøpere får jo ikke vite om de utvidede rettighetene før etter et kjøp. Det ville vært smartere, markedsføringsmessig å ha reklamert for de gode vilkårene litt mer åpent og tilgjengelig. Dette ville kunne være en god måte å skille seg fra mengden ved å reklamere for sine de gode vilkårene. En forklaring for hvorfor man også kan få gunstigere vilkår i en "Shrink-wrap" avtale, vil nok kunne være at man ønsker en mer "rimelig" avtale, i lovens forstand. Selger ønsker ikke at avtalen skal bli kjent urimelig og dermed ugyldig av retten. Det å gi kjøper ekstra rettigheter, kan da være med på å gjøre avtalen mer "rimelig". Videre, kan det nok også være et forsøk fra leverandørens side å standardisere vilkårene ved avtalene sine. Da med tanke på at alle kunder skal behandles likt, uansett hvilket land de måtte ha kjøpt produktet fra. Det er jo ikke nødvendigvis slik at forskjellige land har de samme reglene. Det vil da kunne være besparende å vite at alle kunder er underlagt de samme kontraktsvilkårene. Litt romslige kontraktsvilkår må kanskje til for at kontrakten skal kunne brukes flere land, uten å bli rettstridig i et eller flere av landene.

Shrink-wrap avtaler er dermed også mest brukt av større selskaper, og spesielt når produktet er relativt standardisert. Hvis et produkt blir skreddersydd til en kunde, vil det foreligge en avtale som man har forhandlet seg frem til, i mer eller mindre grad. Det mest typiske eksemplet på en Shrink-wrap avtale, blir da når jeg som privatperson går og kjøper en utgave av Microsoft Office. Det blir da aldri et spørsmål om å forhandle frem en avtale. Ikke vil det være særlig praktisk heller. Microsoft vil ikke kunne ha en representant hos enhver selger av deres produkter. Jeg kjøper så produktet, med mer eller mindre kunnskap om at det medfølger ekstra avtaleklausuler som jeg vil bli kjent med, når jeg åpner pakken, eller installerer programmet. Vi kan se at i en slik avtale, vil kjøperen ikke ha en reell mulighet til å forandre vilkårene i avtalen. Hvis kunden er tilstrekkelig stor, vil nok muligheten til innflytelse på avtalen øke. Det vil være forskjellen i størrelse mellom leverandør og kunde som vil være av interesse. Du må nok være en meget stor kunde, for å kunne forandre må standardvilkår i en avtale med for eksempel Microsoft. Datamaskin leverandøren Dell, vil nok kunne være stor nok til å kunne ha egne avtaler med Microsoft.

3.5.2 Vedtagelse av en "shrink-wrap" avtale.

Avtaleloven bygger som et utgangspunkt på at avtaleslutningen skjer gjennom en eller annen form for forhandling mellom partene. I de fleste tilfeller forekommer det nok allikevel ikke noen form for forhandlinger. Det er da snakk om mindre kjøp av varer og tjenester, hvor man typisk baserer seg på reglene i kjøpsloven. Når man går i butikken og kjøper seg melk og brød, blir det ikke noen foretatt noen forhandlinger om avtalen. Det samme vil være tilfellet for de fleste avtaler man inngår. Det er bare ytterst få avtaler hvor det forekommer en eller annen form for samtale over avtalens innhold.

Det å presentere en kjøper med kontraktsvilkår som følger varen, er meget utbredt. Noe som alle har blitt konfrontert med er vilkårene som blir vist på fjernsynsskjermen før man får se en film man har kjøpt eller leid. Her blir man gjerne vist innskrenkende eller identiske regler som man allerede kan finne i åndsverksloven. Det mest typiske er at det blir satt forbud mot kopiering, offentlig fremføring og fremføring mot betaling. Dette blir nok ofte kun sett på som en påminnelse om den gjeldenderett.

Ved "shrink-Wrap" avtaler et tanken at kjøper aksepterer vilkårene i avtalen ved å bryte forseglingen. Generelt sett, når det gjelder spørsmål om en avtale- eller kontraktsvilkår er vedtatt, vil tidspunktet for når vilkårene ble presentert for kjøperen være viktig. Det klare utgangspunktet er at kjøper må være gjort kjent med kontrakten i sin helhet før eller senest ved kontraheringstidspunktet, for at man vil akseptere at vilkårene blir gjeldende. Det kan dog tenkes unntak fra dette, i begge retninger. Avtalevilkår som blir presentert før avtaleslutningen kan også bli underkjent av retten. Dette vil særlig være tilfellet hvis det er snakk omfattende klausuler, eller vilkår som avviker mye fra den deklarasjoniske bakgrunnsretten eller som er å anse som meget urimelige vilkår. Et eksempel på dette kan vi finne i Rg. 1963 s.634. Dette gjaldt et kjøp av en bil, hvor det i kontrakten var en rekke innskrenkninger i den deklarasjoniske retten. De var plassert under en meget misvisende overskrift, om "garanti- og salgsbestemmelser". Retten kom her frem til at vilkårene ikke kunne anses som vedtatt, mye på grunn av sin kamuflerte natur. Vilårene i seg selv var kanskje ikke så urimelige at de fortjente å bli underkjent, men måten de ble presentert på ved at man prøvde å skjule de for den andre part, ble utslagsgivende. Ett lignende argument kan også brukes ovenfor etikettering. Hvis man

har avtalevilkår man ønsker tatt inn i avtalen, så vil det beste være å presentere disse for den annen part før kontraktinngåelsen. Gjør man ikke det, så taler mye for at de vil bli underkjent av retten.

I enkelte tilfeller, har man valgt å plassere etiketteringen synlig på innpakningen. Dette er et forsøk på å imøtekomme den kritikk man har fått ved at kjøper ikke har hatt mulighet til å gjøre seg kjent med innholdet av avtalen før etter kjøpet. Et problem her er jo at man gjerne ikke har tilstrekkelig plass, så man må bruke liten skrift og/eller være meget kortfattet. I DVD-dommen så ble det hevdet av aktor at logoen DVD, skulle inneholdt kontraktsmessige innskrenkninger i bruken av produktet. Dette ble ikke tatt til følge av retten, som kort avslo dette.⁷¹ At retten kommer til dette standpunkt er ikke overraskende. Når det allerede er tvil om i hvor stor utstrekning man kan godta etikettering, så kan man nok ikke aksepterer at selger heller ikke trenger å legge ved kontrakten, men kun vise til en logo. Kjøper vil jo her ikke være klar over at det finnes en avtale. Det å da kreve at man skal kunne bli bundet av den, faller på sin egen urimelighet. En mulig kjøper har ikke mulighet til å kunne trekke ut innholde i en mulig avtale ut fra en logo som inneholder tre bokstaver, ”DVD”.

I forarbeidene til endringene i åndsverksloven i 1990, utales det;

”Departementet kan her slutte seg til utvalgets forståelse av gjeldende rett, og peker på at dette ikke er til hinder for at etikettering godtas i særlige situasjoner. Normalt vil slike ensidige forbehold imidlertid ikke være gyldige.”⁷²

Vi kan se her at man åpner for at etikettering kan forekomme, men dette vil kun være i helt spesielle tilfeller.

Til grunn for prinsippet om avtaler, ligger det at partene skal bli enige på forhånd hva ens plikter og krav er. Etter at avtalen er inngått, er partene pliktig til å oppfylle sin del av avtalen. Man kan ikke komme med forandringer til avtalen i ettertid. Man kan dog

⁷¹ Se DVD-dommen - avsnitt 30 i vedlagt kopi.

⁷² Jfr. Ot.prp.nr.33 (1989-1990) side 21, annet avsnitt.

komme med tillegg til avtalen, hvis begge parter enes om dette. Det da å presentere nye avtalevilkår først etter at avtalen er inngått, vil da måtte gjennomgå en meget streng sensur, for å kunne stå seg i retten. Det å åpne for en vid adgang til dette, vil jo være meget urimelig for den annen part, og i det store og hele heller ikke gjennomførbart.

Det vil allikevel være noen tilfeller hvor man vil kunne godta at vilkår kan komme til avtalen selv etter vedtakelsen. Et typisk eksempel på dette er når selger, i avtalen viser til et annet dokument. Ofte da kalt, alminnelige leveringsbestemmelser, eller lignende. Disse nye vilkårene vil ofte bli fremmet med ordrebekreftelsen eller ved levering. Et typisk eksempel vil være vilkår om salgspant. Et eksempel på dette kan vi finne i Rt. 1925 s.759. Her ble kjøper presentert med et dokument med selgers leveringsbestemmelser, ved avtaleslutningen. Denne ble heftet på kontrakten, og inneholdt blant annet en klausul om salgspant. Dette ble godtatt av Høyesterett. Mye av bakgrunnen for dette er nok at det ikke er en uvanlig praksis, og det at den ikke var spesielt urimelig for noen av partene.

I en "shrink-wrap" avtale finner man også gjerne en klausul om at man har vedtatt avtalen, og er bundet av den, ved å bryte forseilingen. Poenget med en slik klausul må nok være å prøve å skape et inntrykk av mer legitimitet ovenfor kjøperen. Det er nok lite trolig at en domstol ville legge vekt på en slik klausul. Dette blir en slags sirkelargumentasjon. Hvis retten ikke godtar vedtagelsesformen, så vil ikke da at det står i avtalen at man har godtatt vedtagelsesformen gjøre at avtalen står seg i retten. Man må jo i de fleste tilfeller faktisk bryte forseilingen for å kunne få kjennskap til de nye vilkårene. Som nevnt over, så finner ikke retten i DVD-dommen at det fremkommer på DVD-platen at man er bundet til å bruke autorisert avspillingsutstyr. Retten uttaler videre at hvis merkingen "DVD", som hevdet av påtalemyndigheten, skulle inneholde en slik klausul, så ville den uansett ikke vært kontraktsmessig vedtatt av den tiltalte.⁷³

Det skal sies at i de fleste "Shrink-wrap" avtaler, så har man en mulighet til å returnere varen, hvis man ikke ønsker å vedta avtalen. Et problem med dette er at det kan bli

⁷³ Se vedlagt kopi av DVD-dommen avsnitt 30 annen setning.

kostbart. For det første så har man lagt ut for kjøpet, og det er ikke alltid like lett å få tilbakeført penger, speilet hvis man har kjøpt fra utlandet, for eksempel over internett og har betalt med kredittkort. For det andre så vil man ikke alltid få refundert kostnaden ved å sende produktet tilbake. Da har man påført kjøper en kostnad ved å ikke opplyse om kontraktsvilkår på forhånd. Dette vil også ha likheter med sirkelargumentasjon som nevnt over. Det at man har implementert en måte å komme seg ut av avtalen på, i avtalen, gjør ikke avtalen mer legitim.

Fra et samfunnsmessig syn så vil det nok heller ikke være ønskelig å åpne for en utstrakt bruk av etikettering. Det vil nok være mer hensiktsmessig å ha en lovgivning som forbrukeren kan gjøre seg godt kjent med. Både når det gjelder rettigheter og plikter. Således kan etikettering være egnet til å opplyse om den gjeldende rett, men en utstrakt bruk vanskeliggjøre slutning av avtaler, da man ikke ville være sikker på hva man har bundet seg til.

En utstrakt bruk av etikettering vil også kunne skape praktiske problemer der hvor forbrukeren videreselger varen til en tredjeperson. Utgangspunktet er jo at man ikke kan gi fra seg en større rett enn den man slev har. Tredjeperson vil da gjerne ikke bli gjort kjent med disse vilkårene. Enten fordi de var trykket på forpaktningen, eller vist på et skjermbilde. Det vil således fort kunne oppstå tvil over hvilke kontraktsvilkår som gjelder.

Fra rettspraksis kan nevnes grammofondommene fra RT-1940-450 og RT-1955-536. Høyesterett slo her fast at det var mulig for utgiveren av en grammofonplate å forby kringkasting eller offentlig fremføring av grammofonplaten, uten en nærmere avtale om dette. Grammofonplatene var kjøpt på vanlig vis, det vil si i butikk. Forbudet var trykket på platen. Høyesterett kom i det første tilfelle frem til at rikskringkastingen var å anse som bundet av vilkåret. Det er dog i dag alminnelig antatt at disse dommene er uriktige.

Man må kunne si at gjeldenderett, ikke vil godta avtalevilkår som nevnt i kapittel 3.5, når de blir presentert i en "shrink-wrap" avtale. Spesielt når skepsisen til de to delene hver for seg, er så stor.

3.5.2.1 Innholdsmessige mangler ved "Shrink-wrap" klausuler.

De innholdsmessige manglene ved etikettering vil i all hovedsak være sammenfallende med annen avtaleslutning.

Typisk vil en "Shrink-wrap" klausul som oftest inneholde to hovedtyper av avtalevilkår. For det første har man ofte inntatt punkter om hvilke misligholdsbeføyelser man kan gjøre gjeldende, reklamasjons regler, for hvilket verneting tvister skal føres, med mer. Ikke sjeldent stemmer disse overens med reglene som allerede finnes i lovgivningen. For det andres så inneholder også "Shrink-wrap" klausuler som har til formål å begrense kjøperens rådighetsutøvelse.

Shrink-wrap avtaler vil som andre avtaler være underlagt regler om innholdsmangler som ugyldighetsgrunn. En "shrink-wrap" klausul vil således kunne bli rammet av NL 5-1-2 hvis den blir å anse å stride mot lov eller ærbarhet. Det som i denne sammenheng kan være inntresant, er å se om det kan foreligge ugyldighetsgrunner som følge av avtalen som sådanne.

En avtalen kan, etter avtalelovens § 36, settes helt eller delvis til side, hvis den er urimelig eller i strid med god forretningsskikk å gjøre den gjeldende. Man har sett tilfeller hvor det har vært klausuler som sier at ved eventuelle konflikter, så skal sak reises for en domstol i firmaets hjemstat. For et produkt kjøpt i Norge fra utlandet, så vil nok en norsk domstol sette denne klausulen tilside.

Når en skal se om en avtale er urimelig, så følger det av en helhetsvurdering. Flere mindre urimeligheter, vil således i felleskap likevel medføre urimelighet.

Det kanskje mest nærliggende i denne sammenheng, vil være spørsmålet om avtalen ivaretar begge parter interesser. Særlig da med tanke på de tilfeller hvor en part blir tilgodesett, gjerne på den andres bekostning. Dette problemet som kan bli ytterligere forsterket av "shrink-wrap" avtalens karakter. Avtalen er ensidig opprettet. Det er bare en av partene som kan påvirke innholdet i avtalen. Hvis avtalen da i tillegg favoriserer denne part, vil avtalen fort kunne bli å anse som urimelig etter avtalelovens § 36.

3.5.3 "Click-wrap" avtaler.

Etikettering har forøvrig også mye til felles med såkalte "Web-wrap" eller "Click-wrap" klausuler. Dette er en avart av "shrink-wrap" avtalene, og er en ordning ved kjøp av varer eller tjenester over internett. Mye av likheten ligger i at avtalen eller klausulene er ensidige. Kjøper kan ikke forhandle seg fram til endringer, eller utelate enkelte punkter i kontrakten. Innholde i avtalen er også sammenfallende. Det er imidlertid noen viktige forskjeller. Ved en "web-wrap" avtale blir man opplyst om kontraktsvilkårene før man aksepterer avtalen. Typisk vil dette bli gjort ved at man blir presentert med en rekke vilkår, og anmodet om å lese gjennom kontraktsvilkårene. Nederst på siden vil man typisk ha to valg "Accept" eller "Decline".⁷⁴ I noen tilfeller vil det ikke være mulig å velge "Accept" før man har bladd igjennom vilkårene. Dette for å gjøre kjøper observant på vilkårene, og kan virke som et insitament til å faktisk gjøre seg kjent med dem. Hvis kjøper ikke er villig til å godta vilkårene, så vil man ikke få gjennomført kjøpet. Dette i motsetning til en "shrink-wrap" hvor man som sagt får kjennskap til vilkårene først når man åpner innpakningen.

Når det gjelder spørsmål om slike avtaler kan anses som gyldige etter norsk rett, så ville det før ha vært en viss tvil. Dette er dog nå avklart i den nye E-handelsloven⁷⁵, som regulerer inngåelse av avtaler for elektronisk handel og andre informasjonssamfunnstjenester, jfr. ehandelsloven § 1. Man har her blant annet innført en opplysningsplikt for tjenesteyteren, som han må yte før den elektroniske bestillingen kan gjennomføres, jfr. § 11. Videre skal en tjenesteyter alltid, uten ugrunnet opphold sende en bekreftelse på en eventuell bestilling, jfr. ehandelsloven § 12.

Det vil foreligge de samme begrensninger som man har for andre standardavtaler. For det andre kan det bli spørsmål om det forligger innholdsmessige mangler ved avtalen etter den generelle avtaleretten.

⁷⁴ Se Wagel og Ødegaard - "Opphavsrett i en digital tid" kap. 12

⁷⁵ Lov 2003-05-23 nr. 35: (ehandelsloven).

Ved kjøp av datamaskinprogrammer vil man i noen tilfeller bli presentert med kontraktsvilkår på skjermen etter eller under installasjonen av datamaskinprogrammet. Dette må ikke forveksles ”Click-wrap”. Dette må være likestilt med en shrink-wrap på grunn av tidspunktet for fremleggelsen av klausulene. Det at det ser likt ut, i form av at man kan velge å trykke på ”Accept” eller ”Decline” vil ikke være utslagsgivende. Her vil tidspunktet for presentasjon av kontrakten være avgjørende.

4 Oppsummering.

Det kan stilles spørsmål ved viktig det er å omhandle DVD-dommen, nå som det i nær fremtid vil bli gjort endringer i lovverket som dommen baserer seg på. Jeg ser dommen som viktig, ikke bare på grunn av engasjementet den har skapt. Den har også tydeliggjort utfordringene den teknologiske komplisiteten har skapt for lovgiver og domstolen. Ikke lett for juristen å sette seg inn i sakens faktum, eller for lovgiver å se konsekvensene av for unøyaktige begreper.

Det vil således kunne mange erfaringer å hente fra denne dommen. Dommen fremhever hvilke konsekvenser tvetydige begreper i lovteksten kan få. Dette er noe man kan ta lærdom av i den fremtidige lovgivningen.

5 *Litteraturliste*

Bøker:

Andenæs, Johs – Alminnelig strafferett, utg. 4 – ISBN 82-00-22545-3

Bing, Jon – Rettslige kommunikasjonsprosesser – ISBN 82-00-06089-6

Eckhoff, Torstein – Rettskildelære, utg. 4 – ISBN 82-518-3602-6

Hov, Jon – Avtaleslutning og ugyldighet. – ISBN 82-91060-06-1

Wagel og Ødegaard – Opphavsrett i en digital tid. – ISBN 82-456-0133-0

Wanvik, Guru Wanda – Straffbar hacking – Complex 2/98

Slettan og Øie – Forbrytelse og straff, Lærebok i strafferett – ISBN 82-518-3515-1

Steen, Therese – en fremstilling av ånsdverkloven § 12 første ledd anvendt på litterære verk, samt en legislativ vurdering av digital eksemplarframstilling til privatbruk. - CompLex nr. 1/97 - ISBN 82-518-3551-8

Artikler:

Arendt, Trostein – Shrinkwrap- og clickwrap-avtaler, Lod-1999-058-21

Lloyd, Ian – ”Rettslige aspekter ved etiketteringsavtaler om disposisjonsrett til programmer”. – LoD-1998-054-09

Bing, Jon – Brevbrudd, data og DVD - Lovdata

Bing, Jon – Opphavsrett og EDB - Complex nr.2/85

Selmer, Knut – Hva er ”Data” - Lovdata

Steen, Therese – Eksempelarfremstilling av litterære verk til privat bruk – i en digital verden

Vyrje, Mangnus Stray – “Shrink-Wrap” klausuler – LoR 1986 s. 47-53

– Complex 2/85

Forarbeider:

Ot.prp.nr.46 (2004-2005) - Om lov om endringer i åndsverkloven m.m.

Høringsutkast om forslag til endringer i åndsverkloven m.m. Høringsfrist 25. juni 2003

NOU 2003:27 – Lovtiltak mot datakriminalitet, Delutredning I om Europarådets konvensjon om bekjempelse av kriminalitet som knytter seg til informasjons- og kommunikasjonsteknologi.

Ot.prp.nr.33 (1989 - 1990) – Om lov om endringer i åndsverksloven.

Ot.prp.nr.34 (1987-1988). Om lov om endringer i åndsverkloven m m.doc

Ot.prp.nr.35 (1986 - 1987) – Om endringer i straffeloven (datakriminalitet)

NOU 1985:31 – Datakriminalitet.

NOU 1983:35 – Endringer i åndsverkloven

Ot.prp.nr.4 (1978-1979) - Om lov om endringer i straffeloven

Dommer:

| | |
|------------------|--|
| LB-2003-00731 | - DVD-Jon dommen – Borgarting lagmannsrett |
| TOslo-2002-00507 | - DVD-Jon dommen – Oslo Tingrett |
| Rt-1998-1971 | - Norman Data Defence |
| Lb-1997-01527 | - Norman Data Defence |
| TPBYR-1997-01449 | - Atekst-dommen |
| Rt-1995-35 | - Dekoder dommen 2 |
| Rt-1994-1610 | - Dekoder dommen 1 |
| Rt-1979-1492 | - |
| Rg-1963-634 | - |
| Rt-1955-536 | - Grammofon dommen II |
| Rt-1940-450 | - Grammofon dommen I |
| Rt-1925-759 | - |

Lovregister:

| | |
|------|--|
| 2003 | Lov om visse sider av elektronisk handel og andre informasjonssamfunnstjenester (ehandelsloven) - LOV-2003-05-23-35 |
| | § 1 |
| | § 11 |
| | § 12 |
| 1961 | Lov om opphavsrett til åndsverk m.v. (åndsverkloven) - LOV-1961-05-12-2 |
| | § 2 |
| | § 12 |
| | § 12 annet ledd |
| | § 12 annet ledd d |
| | § 39 g |
| | § 39 h |

1918 Lov om avslutning av avtaler, om fullmakt og om ugyldige viljeserklæringer.
(avtaleloven) - LOV-1918-05-31-4

§ 36

1902 Almindelig borgerlig Straffelov (Straffeloven) - LOV-1902-05-22-10

§ 90 første ledd.

§ 91 første ledd.

§ 145 første ledd.

§ 145 annet ledd

§ 262

§ 270 første ledd nr.2

Annet:

Veiledning med Dr. juris, Jon Bing.

Forelesning av Professor Gideon Parchomovsky - "External perspectives on the DVD-Jon Case" ved institutt for privatrett. 15 september 2004

6 Vedlegg.

6.1 LB-2003-00731 – Borgarting lagmannsrett - DVD-Jon domme

Borgarting lagmannsrett - Dom.

| | |
|--------------------------------|---|
| INSTANS: | Borgarting lagmannsrett - Dom. |
| DATO: | 2003-12-22 |
| PUBLISERT: | LB-2003-00731 |
| STIKKORD: | Datakriminalitet. Bevisbedømmelse. Lovanvendelse. Åndsverksloven §4, §12 og §39i, straffeloven §145 annet ledd. |
| SAMMENDRAG: | <p>En ung gutt hadde i 1999 sammen med andre medvirket til at et program som omgikk Content Scrambling System-beskyttelsen på DVD-plater ble lagt ut på nettet. Han hadde programmert brukergrensesnittet som gjorde programmet tilgjengelig også for personer uten spesiell datakunnskap. Lagmannsretten fant, på samme måte som tingretten, at den programutvikling som hadde funnet sted, ikke var ulovlig. Det som var utført, ble ikke funnet å stride mot reglene i åndsverksloven. Adgangen kunne da ikke sies å være uberettiget i forhold til straffeloven §145 annet ledd. Økokrims anke ble etter dette forkastet.</p> <p>Henvisninger: lov-1902-05-22-10-§145 (Strl §145), lov-1961-05-12-2-§12 (Åvl §12), lov-1961-05-12-2-§39i (Åvl §39i), lov-1961-05-12-2-§4 (Åvl §4).</p> |
| SAKSGANG: | Oslo tingerett TOSLO-2002-00507 - Borgarting lagmannsrett LB-2003-00731 M/02. |
| PARTER: | Den offentlige påtalemyndighet (Førstestatsadvokat Inger Marie Sunde) mot A (Forsvarer: Advokat Halvor Manshaus). |
| FORFATTER: | Lagdommer Wenche Skjæggestad, formann. Kst. lagdommer Endre Stavang. Ekstraordinær lagdommer Hjalmar Austbø. Meddommere: Institusjonssjef Bente Brunvatne. Platearbeider Morten Midtun. Seniorskonsulent Dag Asheim. Høgskolelektor Martin Gilje Jaatun. |
| Henvisninger i teksten: | lov-1902-05-22-10-§35 (Strl §35), lov-1902-05-22-10-§52 (Strl §52), lov-1915-08-13-5-§88 (DI §88) |

1. A er født *.* 1983 og bor i --vei **, Oslo. Han er student, ugift og uten forsørgelsesbyrde.
2. Ved tiltalebeslutning utferdiget av statsadvokatene ved Økokrim, endret to ganger, sist 13 desember 2002, er A satt under tiltale ved Oslo byrett for overtredelse av:

Straffeloven §145 annet jf tredje ledd og fjerde ledd

for ved å ha brutt en beskyttelse eller på lignende måte uberettiget skaffet seg adgang til data som er lagret eller som overføres ved elektroniske eller andre

tekniske midler og ved å ha voldt skade ved erverv eller bruk av slik uberettiget kunnskap, eller å ha medvirket hertil.

Grunnlag er følgende forhold eller medvirkning til dette

I perioden september 1999-24. januar 2000, via Internett fra bopæl i X, deltok A i knekkingen av det tekniske beskyttelsessystemet Content Scrambling System («CSS»), lisensiert av DVD Copy Control Association Inc, for å beskytte DVD-filmer produsert av Motion Pictures Association mot kopiering. En DVD-film er en film som er lagret elektronisk på en DVD-plate. Basert på kunnskap om hemmelig algoritme og spilenøkler inkorporert i CSS, laget A Windows-programmet **DeCSS**. Ved bruk av **DeCSS** fremstilles en ubeskyttet kopi av DVD-filmen. A benyttet **DeCSS** på egne DVD-filmer, og han spredte **DeCSS** flere ganger i flere versjoner via Internett (både) i nevnte periode. Ved det beskrevne forhold skaffet A seg uberettiget adgang til det hemmelige nøkkellageret i CSS. Videre brøt A kopibeskyttelsen på DVD-filmene og skaffet seg og andre adgang til dataene på DVD-platene i ubeskyttet form. Adgangen var uberettiget fordi DVD-filmene var solgt med forutsetning om at brukeren skulle bruke autorisert avspillingsutstyr og respektere kopibeskyttelsen. Tilegnelsen av filmene i ubeskyttet form har voldt skade fordi rettighetshaverne ikke lenger har vern mot uberettiget spredning av filmene.

Almenne hensyn krever påtale.

3. Oslo tingrett avsa 7. januar 2003 dom med slik domsslutning:

- I. A, født *.*.1983, frifinnes.
 - II. Påstand om inndragning tas ikke til følge.
 - III. Saksomkostninger ilegges ikke.
4. Om det nærmere saksforhold og tiltaltes personlige forhold vises til Oslo tingretts dom og lagmannsrettens bemerkninger nedenfor.
 5. Påtalemyndigheten, Økokrim, har i rett tid påanket dommen til Borgarting lagmannsrett. Anken, som gjaldt lovanvendelsen under skyldspørsmålet, saksbehandlingen samt deler av bevisbedømmelsen under skyldspørsmålet, ble henvist til ankeforhandling ved lagmannsrettens beslutning av 17 februar 2003.
 6. Ankeforhandling ble avholdt i tidsrommet 2. til og med 11. desember 2003. To av de fire meddommerne, seniorkonsulent Dag Asheim og høghskolelektor Martin Gilje Jaatun er datafagkyndige og oppnevnt utenfor utvalgene, jf domstoloven §88. Tiltalte og syv vitner avga forklaring. Fire av vitnene ble avhørt som sakkyndige uten oppnevning. Dokumentasjonen fremgår av rettsboken.

Aktors påstand:

1. A, f. *.*.83, dømmes i samsvar med tiltalen til en straff av fengsel i 90 - nitti dager, som gjøres betinget med en prøvetid på 2 - to år, jf strl §52 flg.
2. A, f *.*.83, dømmes til å tåle inndragning av
 - a. Ett stk PC-kabinett Pentium III 500 Mhz (beslag A-2), jf strl §35 annet ledd.

- b. 8 stk CD-rom inneholdende diverse ulisensiert programvare (beslag A-4-6), jf strl §35 annet ledd.
3. A, f *.83, dømmes til å bære sakens omkostninger med kr 20.000 - kronertyvetusen.

Forsvarers påstand:

Anken forkastes.

Lagmannsretten skal bemerke:

7. Etterforskning mot A ble igangsatt i januar 2000 etter at Motion Picture Association og DVD Copy Control Association Inc., (heretter kalt DVD CCA) hadde inngitt anmeldelse til Økokrim. Stiftelsen DVD CCA ble formelt dannet i slutten av 1999. Formålet var å administrere en kontrollordning som bl.a. skulle hindre piratkopiering av DVD-filmer. Det er på det rene at piratkopiering er et stort problem for filmbransjen. Filmbransjen lanserer de fleste filmer til ulik tid på de forskjellige markeder. Økonomisk sett er det viktig for filmselskapene å bestemme over i hvilken rekkefølge markedene får tilgang til den enkelte film. I følge vitnet Marsha King, Warner Home Video, koster det i gjennomsnitt medlemmene av Motion Picture Association, 88 millioner USD å produsere og markedsføre en spillefilm. Bare ca 20% av filmene går med overskudd. Video- og DVD-markedet har etter hvert blitt de markeder som genererer de største inntektene. For Warner Brothers del utgjør inntekten fra disse markeder ca 60%. DVD utgjør ca 80% av dette.
8. Sonekoding er et viktig virkemiddel for selskapene. Det har vært problematisk å utgi filmer på alle markeder samtidig. Blant annet var det tidligere vanskelig å lage tilstrekkelig antall « masterkopier ». Filmene må i mange land dubbes eller tekstes. Filmselskapene ønsker også ofte å se an om filmen selger i USA, for tradisjonelt er det retningsgivende for salgsmulighetene også på andre kontinenter. Endelig kan sensur i det enkelte land skape problemer for samtidig utgivelse.
9. Blant annet det faktum at filmene lanseres til forskjellig tid, har skapt et marked for piratkopiering. Denne form for kopiering har lenge vært et stort og kostbart problem for filmbransjen. Det er utarbeidet svært rigorøse retningslinjer for hvordan selskapene selv behandler sine filmkopier. Det alvorligste som kan skje, er at det foretas uautorisert kopiering av en film som ennå ikke er sluppet på alle markeder. Mange illegale metoder har vært tatt i bruk, og det har bl.a. blitt oppdaget kopiering ved hjelp av håndholdte videokameraer under filmfremvisninger. Denne metoden gir imidlertid en kopi av dårligere kvalitet enn originalen.
10. DVD-mediet er digitalt, hvilket gjør det mulig å lage perfekte kopier hvis man kommer til innholdet på DVD-plater. Av åpenbare grunner var derfor filmselskapene innledningsvis svært reserverte i forhold til å benytte DVD-plater som medium før det var mulig å beskytte innholdet mot kopiering. På denne bakgrunn ble CSS - Content Scrambling System - utviklet.
11. Etter avtale mellom de største filmselskapene i USA og DVD CCA, ble det utarbeidet en lisensieringsordning. DVD-filmer skulle bare kunne spilles av på spillere med Content Scrambling System som var produsert etter lisens gitt av

DVD CCA. Lisensregimet var åpent i den forstand at hvem som helst kunne få lisens til å produsere spillere mot å betale en årlig avgift, samt mot å forplikte seg til å følge et bestemt regelverk. Lisenshavere fikk utlevert en eller to spillernøkler og forpliktet seg til å beskytte denne/disse. At man ikke vet sikkert om det er en eller to spillernøkler som utleveres, skyldes at DVD CCA ikke har vært villig til å utlevere programmet til Økokrims sakkyndige vitner fordi spillernøklerne blir ansett for å være forretningshemmeligheter. Hvis en DVD-spiller eller et avspillingsprogram på en PC med DVD-stasjon ikke er slik innrettet at nøkkelen/nøklerne er godt nok beskyttet mot kopiering, vil lisenshaveren i henhold til lisensvilkårene kunne pålegges å betale et større erstatningsbeløp til DVD CCA. I tillegg til kryptering består systemet av en autentiseringsmekanisme som skal hindre at uautoriserte spillere får tilgang til nøkkelmaterialet på DVD-platen. Autentiseringen innebærer at komponentene må kjenne hverandre igjen før avspilling kan skje.

12. Det er på det rene at krypteringsalgoritmen i CSS er svak. På det tidspunkt filmbransjen og forbrukerelektronikkbransjen gikk sammen om å utarbeide et system for sikker distribusjon av innholdet på en DVD-plate, forbød den amerikanske eksportlovgivningen at det ble brukt mer enn 40 bit kryptering. Det byr ikke på alt for store problemer å knekke en slik kryptering. Lagmannsretten legger til grunn at en relativt sikker kryptering må være på i alle fall 64 bit. Bankene sikrer informasjon over nettet med 128 bit, som regnes som svært sikkert. Da vitnet Stevenson i slutten av november 1999 foretok en kryptoanalyse av CSS-algoritmen med sikte på å få ut filmnøklerne, viste det seg at den i realiteten kun representerte en effektiv beskyttelse tilsvarende 16 bit. Krypteringen må etter dette betegnes som svært svak. Basert på denne kryptoanalysen laget for øvrig Stevenson et program som kunne knekke en vilkårlig CSS nøkkel på mindre enn ett sekund, noe som tillot avspilling av DVD-plater på ulisensierte DVD-spillere uten bruk av spillernøkler overhodet.
13. Som gjennomgått ovenfor, er piratkopiering et meget stort problem for både film- og musikkbransjen. I Sør-Øst Asia er det lokalisert fabrikker som produserer DVD-plater legalt om dagen og hvor de samme lokalene brukes til illegal produksjon om natten. Med spesialutstyr er det også mulig å kopiere en DVD-plate direkte slik at også krypteringen blir liggende på piratkopien. Begge disse metoder gir kopier av like høy kvalitet som originalen. I International Intellectual Property Alliance 2001 Special 301 Report vedrørende Taiwan, ble det rapportert at et økende antall fabrikker engasjerte seg i uautorisert produksjon av digitale medieprodukter. Produksjonskapasiteten var astronomiske 1,8 milliarder plater pr år.
14. Kopiering av filmer over Internett var derimot ikke særlig praktisk i 1999. Overføringskapasiteten var ikke god nok, idet det tok ca 12 døgn å overføre en hel ukomprimert spillefilm over ISDN-linje. Bredbånd var ikke særlig utbredt. En spillefilm opptok inntil 8 gigabytes i lagringsplass, hvilket var mye med datidens lagringskapasitet på PC-er. Kopiering var heller ikke særlig praktisk. En DVD-brenner kostet i 1999 ca kr 20.000, og DVD-plater for brenning hadde for liten kapasitet til en hel film, i tillegg til at de var vanskelig å få kjøpt. Kopiering til vanlige CD-er var enklere og rimeligere, men en film opptok lagringsplass på minimum 3 - 4 CD-er, og kvaliteten ble dårligere enn på originalen. Verken prismessig eller kvalitetsmessig var det altså noe særlig poeng i kopiering. Lagmannsretten legger derfor til grunn at piratkopiering ikke

har vært noe primærmål med utvikling av en spiller utenfor DVD CCA-systemet. Dette fremgår for øvrig av de fremlagte samtalelogger hvor bl.a. A uttaler seg svært negativt om piratkopiering.

15. De fremlagte samtalelogger viser at det var flere uavhengige grupper og enkeltpersoner med datakunnskaper som engasjerte seg i å utvikle en DVD-spiller utenfor DVD CCA lisensieringssystemet. Den første som etter de fremlagte opplysninger lyktes med å omgå kodingen, var en russer kjent som « Landy ». I slutten av april 1999 lyktes han etter det opplyste med å tappe dekypterte filmdata fra en Power DVD-spiller mens filmen ble avspilt.
16. Årsakene til at mange ønsket å utvikle en uavhengig DVD-spiller var flere. Lagmannsretten legger til grunn at knekking av krypteringen i seg selv representerte en utfordring, men det var også andre grunner. Mange forbrukere likte dårlig sonekontrollsystemet. Dette systemet sikret at filmselskapene kunne prise filmene forskjellig i de forskjellige markedene. DVD-filmer var ca 50% billigere i USA enn i Europa. I tillegg var det flere forhandlere i Norge som kjøpte inn filmer beregnet på andre markedene. Alle DVD-covere har soneangivelse, men opplysningen var vanskelig å oppdage for en vanlig forbruker, og det må legges til grunn at det ikke ble gitt opplysninger om sonekode av forhandleren. Det medførte at norske brukere kunne risikere å kjøpe en DVD-film av en norsk forhandler som ikke lot seg avspille på det utstyret de hadde. Det er fremlagt eksempler på dette med filmer innkjøpt hos Akers Mic i Oslo og hos en forhandler i Arendal. Samme problem fikk personer som hadde kjøpt DVD-filmer i utlandet for avspilling i Norge. Dette problemet har etter hvert blitt så åpenbart at man i dag kan få kjøpt lisensierte spillere med programmer som, i strid med lisensen, eliminerer sonekodingen.
17. Lagmannsretten legger til grunn at ikke alle produsenter av software kunne akseptere de lisensvilkår som DVD CCA fastsatte. Produsenter av programmer under operativsystemet Linux baserer seg på prinsippet om åpen kildekode, slik at andre kan se hvordan programmene er bygget opp. Formålet med dette er å oppmuntre andre til å videreutvikle programmene. Høsten 1999 fantes det ingen DVD-spiller under dette systemet, og lisens fra DVD CCA var ut fra filosofien om åpen kildekode ikke mulig å oppnå.
18. A var en av mange som ventet på at det skulle utvikles en spiller under operativsystemet Linux. Gjennom samtalekanalen Relay Chat (heretter kalt IRC), kom han i kontakt med likesinnede. 11 september 1999 hadde han en samtale med « mdx » om hvordan man kunne finne krypteringsalgoritmen i CSS ved å finne frem til en programvarebasert spiller som hadde dårlig beskyttelse av spillernøkklene. Av en samtale mellom de samme 22 september, opplyser « mdx » at « the nomad » hadde funnet programkoden for dekrypteringsalgoritmen i CSS, og at « mdx » nå sendte denne til A. « The nomad » skulle ha funnet dekrypteringsalgoritmen gjennom såkalt omvendt utvikling av en Xing DVD-spiller hvor spillernøkklene lå mer eller mindre åpent tilgjengelig. På denne måten fikk han ut informasjon som gjorde ham i stand til å lage koden CSS_scramble.cpp. Det fremgår av samtalelogger datert 4. november 1999 og 25. november 1999 at « the nomad » utførte den omvendte utviklingen på en Xing-spiller han har betegnet som ikke lovlig. Slik saken er opplyst for lagmannsretten, var imidlertid dette ukjent for A frem til 4 november.

19. Når det gjelder autentiseringskoden, legger lagmannsretten til grunn at « the nomad » fikk denne via e-postlisten LiVid (Linux Video) på Internett, og at den var utarbeidet av Derek Fawcus. Det fremgår av en LiVid-posting datert 6 oktober 1999 at Derek Fawcus på denne datoen leste igjennom kildekoden til **DeCSS**, og sammenlignet den med sin autentiseringspakke. Det fremgår videre: « Forfatterne har tatt den nesten ordrett - det eneste de gjorde var å fjerne min copyright-topptekst og et avsnitt med kommentar og gi funksjonene nye navn ». Navnet var CSS_auth.cpp.
20. Det må etter dette legges til grunn at det programmet A senere programmerte, brukergrensesnittet (Graphical User Interface), besto av « the nomad »s dekrypteringsalgoritme og Derek Fawcus' autentiseringspakke. Utarbeidelsen av et brukergrensesnitt gjorde programmet tilgjengelig også for brukere uten spesialkunnskap om programmering. Programmet ble første gang publisert på Internett 6 oktober 1999, etter at A hadde testet det ut på filmen « The Matrix ». I den forbindelse lastet han ned ca 2,5% - 200 megabytes - av filmen til harddisken på sin PC. Denne nedlastingen er det eneste A har lagret av film på sin PC.
21. Programmet, **DeCSS**, ble etter hvert forbedret og lagt ut i flere versjoner. Siste versjon ble etter det som er opplyst, lagt ut 9 november 1999. Programmet virket under operativsystemene Microsoft Windows 98 og Windows 2000.
22. A har anført at hans hensikt med å lage programmet var å bidra til utviklingen av en Linux spiller. Lagmannsretten legger dette til grunn, og finner at årsaken til at programmet som ble lagt ut, var et program som virket på Microsoft Windows operativsystem, var at det på det daværende tidspunkt ikke var noen ferdig utarbeidet støtte for filsystemet UDF på Linux. A hadde ikke kunnskaper nok om Linux til å bidra i dette arbeidet. Vitnet Stevenson uttalte at det arbeidet A utførte, gjorde det lettere for andre å teste ut sine komponenter, slik at man kom nærmere utviklingen av en Linux-spiller. Ved en feil fra As side ble også kildekoden til **DeCSS** gjort tilgjengelig på Internett den 6 oktober 1999. Den ble trukket tilbake samme dag. Kildekoden ville han i utgangspunktet holde hemmelig, fordi han ellers var redd for at Xing-nøklerne ville bli trukket tilbake. Skjedde det, ville **DeCSS** slutte å virke. Imidlertid gjorde en anonym kilde koden tilgjengelig igjen på LiVid den 25 oktober. Det fremgår av utskrift av samtaleloggen på denne dato at A i samtale med « the nomad » var irritert over at koden ble « sluppet », men at de på dette tidspunkt hadde annen tilgang til flere nøkler, slik at det ikke spilte noen praktisk rolle. Brian Demsky, som lastet ned kildekoden den 6 oktober, hadde nemlig i mellomtiden laget et program som fant frem til spillernøkler. Denne teknologien var ikke A kjent med, men han videreformidlet spillernøkler til « the nomad », som testet dem ut. Det er også på det rene at Frank Stevenson lastet ned kildekoden den 25. oktober. Han laget et program som helt eliminerte behovet for kunnskap om spillernøkler.
23. A er tiltalt for overtredelse av straffeloven §145 annet, tredje og fjerde ledd. Bestemmelsen rammer den som uberettiget bryter en beskyttelse eller på annen lignende måte skaffer seg adgang til data eller programutrustning som er lagret eller som overføres ved elektroniske eller andre tekniske midler. Bestemmelsen er plassert i straffelovens kapittel 13 som omhandler forbrytelser mot den almindelige orden og fred.

24. Spørsmålet blir først hva som ligger i uttrykket « data ». Lagmannsretten legger til grunn at i denne saken må uttrykket omfatte både filmen og Content Scrambling System-programmet. Forstått slik kan det ikke være tvilsomt at saken omhandler « data » i lovens forstand.
25. Det neste spørsmålet blir hva som ligger i uttrykket « uberettiget ». A har kjøpt alle sine DVD-filmer på regulær måte, og har rett til å avspille dem. Skal de kunne avspilles, må filmene dekrypteres. Forutsetningen for produsenten var imidlertid at filmene i kryptert stand skulle være intakt etter avspillingen, mens As program **DeCSS** tillater lagring av filmene i ukryptert stand på harddisk. En lagret film kan mangfoldiggjøres, f.eks. ved at den brennes på en DVD-plate eller på CD-plater, og det var nettopp dette krypteringen skulle forhindre. Lagmannsretten har ovenfor lagt til grunn at A ikke selv har lagret film for senere kopiering på sin harddisk, men det må likevel tas standpunkt til om det å skaffe seg en slik mulighet i tillegg til avspillingsmuligheten, er uberettiget. I forarbeidene, [Ot.prp.nr.35](#) (1986-1987) Om endringer i straffeloven fremgår det på side 20 nederst:
27. « Ved at « på lignende måte » er føyd til, blir tolkningen av vilkåret om å bryte en beskyttelse ikke så avgjørende. Poenget er at §145 bare skal ramme tilfelle hvor det å skaffe seg adgang til data må karakteriseres som kvalifisert uberettiget. »
28. Ordlyden i §145, sammenholdt med at enhver bruk av **DeCSS** innebærer at det fremstilles en ubeskyttet versjon av de krypterte filmdataene som lagres på brukerens harddisk, taler for at det må påvises et grunnlag som gjør bruken av **DeCSS** rettmessig. En slik hjemmel er åndsverksloven §12 som gir rett til eksemplarframstilling. Ordlyden tyder på at retten er ukvalifisert, men det fremgår av motivene at bestemmelsen må tolkes innskrenkende, se uttalelsene i Ot.prp.nr.15 (1994-1995) Om lov om endringer i åndsverksloven med mer side 38 annen spalte nederst. Til belysning av vurderingstemaet sies:
30. « Hvor stor del av et verk og antall eksemplarer som kan fremstilles, vil bero på omstendigheter i det konkrete tilfelle - bl.a. hva slags verk det er tale om, verkets omfang, hvor stor del av verket som gjengis på eksemplaret, arten av det eksemplar som fremstilles og om eksemplaret gjengir verket i samme form som gjengivelsen det fremstilles fra, og hva slags bruk det tas sikte på. For eksempel vil det normalt ikke være adgang til for personlig bruk å fremstille selv én enkelt kopi av en hel bok, eller et helt tidsskrift som er å få i handelen? ».
31. Slik lagmannsretten ser det, er det en vesensforskjell mellom å kopiere en spillefilm og å kopiere et helt tidsskrift eller en hel bok. Spillefilmen er lagret på et medium som er utsatt for å få skader, f.eks. riper, hakk og sprekker, mens en bok eller et tidsskrift kan leses om og om igjen uten at det går ut over kvaliteten. Lagmannsretten legger til grunn at en DVD-plate er så utsatt for å få skader at kjøperen må være berettiget til å ta en kopi, for eksempel av en film han er spesielt interessert i å bevare. Det kan ikke sees at bruken av **DeCSS** utgjør noen stor fare for illegal eksemplarframstilling av DVD-plater i konkurranse med filmselskapene. Forarbeidene og Bernkonvensjonen art. 9 gir anvisning på en

interesseavveining, men i denne saken er det tolkningen av åndsverksloven §12 som ledd i en straffbarhetsvurdering som er temaet, og i en slik sammenheng må den ubetingede form ordlyden har fått, etter lagmannsrettens vurdering, tillegges stor vekt.

32. Det neste spørsmål blir om bruk av **DeCSS** likevel er rettsstridig fordi filmene selges med forbud mot kopiering. Forbudet fremgår av coveret, men det må legges til grunn at det ikke finnes noen standardisert tekst som kan gjenfinnes på alle covere. Teksten er oftest på engelsk, men kan også være på et annet språk, f.eks. fransk. Teksten er vanskelig tilgjengelig, og den er skrevet med svært liten skrift.
33. Et forbehold om forbud mot kopiering ville beskjære forbrukerens rettigheter i forhold til åndsverksloven §12, som tillater at enkelte eksemplar av et offentliggjort verk fremstilles til privat bruk når slik fremstilling ikke skjer i ervervsøyemed. Lagmannsretten legger til grunn at ensidige forbehold mot bruk som er tillatt etter åndsverksloven ikke kan anses for å være gyldige. Det vises til [NOU 1983:35](#) Endringer i åndsverksloven m.v. hvor det på side 63, første spalte heter:

35. « Utvalget mener at det som gjeldende rett må legges til grunn at ensidige forbehold mot bruk som er tillatt etter åndsverksloven, i alminnelighet ikke kan anses gyldige. Dette standpunkt støttes av reelle hensyn. Slike forbehold synes å kunne sammenlignes med privat lovgivningsvirksomhet som lett kan forrykke den interesseavveining som loven bygger på. Dette synspunkt har i særlig grad gyldighet overfor forbehold knyttet til eksemplar av åndsverk som er fremstilt som masseartikler. For at private forbehold skal være gyldige, må utgangspunktet være at de er kontraktsmessig vedtatte. »
36. Lagmannsretten kan heller ikke se at det fremgår noe sted på DVD-platens cover at A var bundet til kun å bruke autorisert avspillingsutstyr. Hvis det skulle være slik som anført av påtalemyndigheten at denne forutsetning fremgår av merkingen « DVD » på coveret, kan heller ikke denne forutsetning anses for å være kontraktsmessig vedtatt av forbrukeren.
37. Spørsmålet blir dernest om selve dekrypteringsprogrammet var skaffet til veie på ulovlig vis. Hvis det kan påvises, må det tas standpunkt til om dette gjør at adgangen til dataene blir uberettiget.
38. Påtalemyndigheten har for det første anført at den omvendte utviklingen eller dekompileringen som « the nomad » utførte, ikke var omfattende nok til å kunne betegnes som omvendt utvikling. Det han gjorde var å dissekere programmet, såkalt dekompilering. Lagmannsretten kan ikke se at dette er noe poeng i saken. I Ot.prp.nr.84 (1991-1992) Om lov om endringer i lov 12 mai 1961 nr 2 om opphavsrett til åndsverk m.v. og i enkelte andre lover som følge av EØS-avtalen, står det i punkt 3.4.6.3. Merknader til endringsforslaget, bl.a. følgende:

40. « Datamaskinprogrammer fra forskjellige produsenter opererer ofte med ulike standarder. Et program i såkalt objektversjon (maskinkode) vil ikke avsløre ideer eller prinsipper for erververen, og man er derfor avhengig av å kunne foreta en omvendt utvikling av programmets objektversjon til en kildeversjon for å kunne forstå programmets bakenforliggende logikk. »

42. « En annen metode er å foreta såkalt omvendt utvikling, eller « dekompilering », som direktivet benevner det. Dekompilering innebærer at man oversetter datamaskinprogrammets maskinlesbare kode tilbake til skriftlig kildekode, eller noe som tilsvarer den opprinnelige kildekode. Herfra kan man da foreta den nevnte analyse av grensesnittet og de prinsipper som ligger bak. »
43. Slik lagmannsretten forstår dette, er « dekompilering » og « omvendt utvikling » synonymer slik uttrykkene er anvendt i [Ot.prp.nr.84](#) (1991-1992).
44. Utgangspunktet etter åndsverksloven §4 er at en opphavsmann ikke kan sette seg imot at andre benytter hans åndsverk på en slik måte at nye og selvstendige verk oppstår. Åndsverksloven §39i gir hjemmel for å fremstille eksemplar av en datamaskins kode og oversette kodens form når dette er en forutsetning for å skaffe til veie de opplysninger som er nødvendige for å oppnå funksjonelt samvirke mellom et selvstendig utviklet datamaskinprogram og andre programmer, dersom handlingen utføres av en person som har rett til å bruke et eksemplar av et program, opplysningene ikke tidligere har vært lett tilgjengelige og handlingene er begrenset til de deler av det opprinnelige program som er nødvendige for å oppnå funksjonelt samvirke.
45. I den sakkyndige rapporten som er fremlagt i det faktiske utdraget, fremgår det på side 41:
47. « Den metoden som tilsynelatende oftest blir satt i forbindelse med omvendt utvikling er det som kalles dekompilering av datamaskinprogrammets objektkode. Dette er en prosess som skal forsøke å omforme objektkoden til noe som er tilnærmet kildekode på et høyere nivå. Man identifiserer de enkelte instruksjoner i programmet og setter rekker av disse sammen til funksjonsbeskrivelser på et høyere nivå. Man har ingen sikker metode for å komme fram til en nøyaktig representasjon av den originale kildekoden til et program, men vil likevel få meget god kjennskap til de prinsipper som ligger til grunn for utformingen av programmet. Arbeidet med å omarbeide de faktiske maskininstruksjoner i objektkoden til en representasjon av kildekoden kan regnes inn under den delen av omvendt utvikling som vi har valgt å kalle rekonstruksjon av design. »
48. Lagmannsretten legger til grunn at det som ble utført av « the nomad », var en omvendt utvikling av algoritmen og spillernøkklene. Ved å gjøre bruk av den informasjonen han fikk ut av Xing-spillere og Fawcus' autentiseringskode, var han i stand til å skape et nytt program, og oppnå funksjonelt samvirke med DVD-platen. Opplysningene var ikke tilgjengelige for ham fra andre kilder. En eventuell lisens fra DVD CCA påla taushetsplikt om spillernøkler etc., og med filosofien om åpen kildekode i LiVid-miljøet var det en umulighet å underskrive et slikt taushetsløfte. Det program som ble laget svarte ikke i vesentlig grad til det opprinnelige, og opphavsretten til det opprinnelige programmet ble dermed ikke krenket. Om « the nomad » gjorde mer enn det som var nødvendig for å oppnå funksjonelt samvirke, er ikke etterforsket. Det må da legges til grunn at dette vilkår ikke er krenket. Det faktum at han gjorde bruk av Fawcus' autentiseringskode taler under enhver omstendighet for at det bare var de

nødvendige deler som ble omvendt utviklet fra Xing-spilleren. Det er usikkert om « the nomad » hadde lovlig adgang til det spillerprogrammet informasjonen ble hentet ut fra. Dette punkt blir nærmere gjennomgått nedenfor. Det er imidlertid As forhold som er oppe til pådømmelse, og han fikk ikke kjennskap til at « the nomad » antagelig ikke eide et lovlig eksemplar av Xing-spilleren før 4 november 1999. Da hadde **DeCSS** ligget ute på Internett siden 6 oktober 1999. Koden var også ved en feil offentliggjort, og det må da antas at programmet var kjent i de kretser som interesserte seg spesielt for slike spørsmål, bl.a. LiVid-miljøet.

49. Påtalemyndigheten anfører at dekompileringen ble foretatt på et ulovlig eksemplar. Det er i strid med reglene i åndsverksloven. Beviset for at eksemplaret av Xing-spilleren var ulovlig, skal være to uttalelser i IRC-loggen. Den 4 november 1999 uttaler f.eks. « the nomad »:

51. « og det er nettopp derfor jeg foretrekker å forbli anonym, jeg eier ingen lovlig kopi av xingdvd ».
52. Lagmannsretten kan ikke se at påtalemyndighetens bevisbyrde er oppfylt når det gjelder å klarlegge eierforholdet til Xing-spilleren. Det vises til at det programmet det er tale om eierforholdet til, er et program for avspilling av DVD-filmer på en PC, og slike programmer er rimelige i innkjøp. Det er derfor liten grunn til å foreta eksperimenter på en piratkopi. Videre fremgår det flere steder i samtaleloggene, blant annet i logg av 3 november 2000, at « the nomad » ikke har noen kunnskap om hvilke regler som gjaldt for omvendt utvikling. « The nomad » er etter det som er opplyst tysk, og kunne da forholdsvis enkelt ha vært avhørt av tysk politi på vegne av Økokrim, hvis de opplysninger man fant i samtaleloggen ble ansett for å være av avgjørende betydning.
53. Lagmannsretten finner for sin del, som nevnt ovenfor, at dette ikke er et punkt av betydning for As straffbarhet, i og med at opplysningene, hvis de medfører riktighet, først fremkom nesten en måned etter at A hadde publisert **DeCSS** på Internett.
54. For øvrig kan man etter lagmannsrettens syn neppe forlange at den da 15-årige A skulle ha satt seg inn i åndsverkslovens regler om omvendt utvikling. Lagmannsretten viser til at det ikke var ham som utførte dette arbeidet, bl.a. fordi han ikke hadde tilstrekkelige kunnskaper. Regelverket rundt det hadde han da etter lagmannsrettens syn ingen foranledning til å undersøke. At han hadde svært begrensede kunnskaper på området fremgår for øvrig av en samtalelogg mellom ham og Brian Demsky den 9 oktober 1999. Han blir da spurt av Demsky om han har noen ide om hvor legal den omvendte utviklingen var. Han svarer: « som i hvor? som om han gjorde det i et land der dette er tillatt? » Brian Demsky forklarer at han mener om den omvendte utviklingen var forskjellig nok til ikke å bryte opphavsrettslover. A svarer: « Forskjellig nok? »
55. Lagmannsretten må dernest ta stilling til om tilegnelsen av spillernøklene i seg selv var uberettiget. Påtalemyndigheten har anført at dette kun er rettighetsadministrative data som ikke var ment for innsyn fra forbruker. Lagmannsretten kan ikke se at denne delen av det som er lagret på DVD-platen nyter særskilt vern. Nøkkellageret representerer beskyttelsen, og vurderingen av hva som kan anses som uberettiget i forhold til straffeloven §145 annet ledd må,

slik lagmannsretten ser det, knyttes til adgangen til selve filmen. A har kun undersøkt om nøklene fra « the nomad »s kode fungerte på enkelte filmer. De øvrige nøklene er ikke anvendt. For øvrig har, som tidligere nevnt, Frank Stevenson utviklet og offentliggjort et program som helt overflødiggjorde kunnskap om nøklene.

56. Det bemerkes for øvrig at det faktum at beskyttelsessystemet ble kompromittert snarere skyldes at systemet var utilstrekkelig enn at forsøkene var spesielt iherdige. Stevenson betegnet systemets sikkerhet som svært lav, og det sier seg selv at et slikt system lettere vil bli utsatt for forsøk på knekking enn systemer som i utgangspunktet virker robuste.
57. Lagmannsretten legger etter dette til grunn at da A programmerte brukergrensesnittet til **DeCSS**, hadde han ikke noen grunn til å tro at den omvendte utvikling eller dekompilering som var foretatt av « the nomad », ikke var lovlig. Lagmannsretten konkluderer etter dette med at adgangen til dataene ikke kan anses som uberettiget.
58. De to siste spørsmål lagmannsretten må ta standpunkt til, er om A kan straffes for medvirkning eller forsøk på medvirkning til andres bruk av programmet **DeCSS**.
59. Lagmannsretten finner, på samme måte som tingretten, at det ikke er ført noe bevis for at andre har brukt **DeCSS** på ulovlig ervervede DVD-filmer. A kan da ikke straffes for medvirkning til bruk av programmet.
60. Spørsmålet blir så om han kan dømmes for forsøk på medvirkning ved at han har offentliggjort et program som gjør det mulig for andre å få uberettiget adgang til dekrypterte DVD-filmer.
61. Som tingretten, viser lagmannsretten til Erling Johannes Husabø, Straffansvarets periferi - Medvirkning, forsøk, førebuing (1999) side 100 hvor forfatteren tar utgangspunkt i følgende problemstilling: « Nær sagt ei kvar vare kan bli nytta som middel til eit brotsverk. Visse vareslag medfører jamvel ein påreknelig fare for å bli brukt slik. Men like fullt er det semje om at straffansvar normalt er utelukka både for produsent og selger. » Forfatteren viser til at det å omsette f.eks. våpen og medisiner er eksempler på tillatt risiko. Så lenge varene tjener et lovlig formål, er ikke problemet så mye å begrunne straffrihet, men eventuelt å begrunne at salg til andre kan utløse medvirkeransvar.
62. Lagmannsretten har tidligere lagt til grunn at As hensikt med å gjøre **DeCSS** tilgjengelig på Internett var å medvirke til at det ble laget en DVD-spiller for Linux. I henhold til filosofien om åpen kildekode kunne da andre teste programmet og videreutvikle det. Det er lite som tyder på at han ved publiseringen av programmet ønsket å gjøre det lettere for andre å kopiere og å distribuere DVD-filmer, selv om han selvsagt må ha vært klar over at programmet kunne misbrukes. At distribusjon og kopiering var upraktisk i 1999 er gjennomgått ovenfor. I tillegg viser samtalelogger, som tidligere nevnt, at A ikke hadde mye til overs for piratkopiering. Lagmannsretten kan etter dette ikke se at det er ført bevis for at A ved å legge **DeCSS** ut på Internett har forsøkt å medvirke til andres piratkopiering av spillefilmer. At programmet kan misbrukes endrer ikke denne vurdering.
63. **Anken blir etter dette å forkaste.**

64. Spørsmålet om inndragning og spørsmålet om saksomkostninger er det da ikke aktuelt å behandle.

65. Dommen er enstemmig.

66. Slutning:

Anken forkastes.

A

B